НАРЪЧНИК

Наръчник по европейско право в областта на защитата на данните

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Ръкописът на този наръчник е завършен през април 2014 г.
Актуализираните версии на наръчника ще бъдат достъпни на уебсайта на Агенцията на Европейския съюз за основните права (FRA): fra.europa.eu, на уебсайта на Съвета на Европа-coe.int/dataprotection и на уебсайта на Европейския съд по правата на човека в раздел „Съдебна практика“ („Case-Law“) на адрес: echr.coe.int.

Europe Direct е услуга, предназначена да ви помогне да намерите отговори на въпросите, които си задавате за Европейския съюз.

Единен безплатен номер (*):

00 800 6 7 8 9 10 11

(*) Информацията, както и повечето обаждания са безплатни (възможно е обажданията от мрежата на някои оператори, от обществени телефони или от хотели да бъдат таксувани).

Снимка (заглавна страница и вътре): © iStockphoto

Повече информация относно Еворейския съюз е налична в Интернет на (http://europa.eu).

Информация относно използваните източници може да бъде намерена в края на този материал.

Люксембург: Служба за публикации на Европейския съюз, 2014 г.

ISBN 978-92-871-9950-8 (CE)
ISBN 978-92-9239-325-0 (FRA)
doi:10.2811/53167

Printed in Belgium

Принтирано на обработена нехлорирана рециклирана хартия (PCF)

Наръчник по европейско право в областта на защитата на данните

Предговор

Наръчникът по европейско право в областта на защитата на данните е изготвен съвместно от Агенцията на Европейския съюз за основните права (АОП) и Съвета на Европа заедно със Секретариата на Европейския съд по правата на човека. Това е третият от поредицата правни наръчници, изготвени съвместно от АОПи Съвета на Европа. През март 2011 г. беше публикуван първи Наръчник по европейско право в областта на дискриминацията, а през юни 2013 г. — втори Наръчник по европейското право в областта на предоставянето на убежище, границите и имиграцията.

Решихме да продължим нашето сътрудничество по един много актуален въпрос, който ежедневно засяга всички нас, а именно защитата на личните данни. Европа се ползва от една от най-защитените системи в тази сфера, която се основава на Конвенция № 108 на Съвета на Европа и на актовете на Европейския съюз (ЕС), както и на съдебната практика на Европейския съд по правата на човека (ЕСПЧ) и на Съда на Европейския съюз (СЕС).

Целта на този наръчник е да се повиши информираността и да се подобри познаването на правилата за защита на данните в държавите членки на Европейския съюз и на Съвета на Европа, като той служи като основният отправен ориентир, към който читателите могат да се обърнат за справка. Той е предназначен за практикуващи юристи, които не са специализирани в тази област, за съдии, национални органи за защита на данните и други лица, работещи в областта на защитата на данните.

С влизането в сила на Договора от Лисабон през декември 2009 г., Хартата на основните права на ЕСпридоби правнообвързващ характер и с това правото на защита на личните данни беше издигнато до статута на отделно основно право. По-доброто разбиране на Конвенция № 108 на Съвета на Европа и на актовете на Европейския съюз (ЕС), които проправиха пътя за защитата на данните в Европа, както и на съдебната практика на СЕС, и наЕСПЧ, е от решаващо значение за защитата на това основно право.

Бихме искали да благодарим на Института по човешки права “Ludwig Boltzmann” за неговия принос при изготвянето на този наръчник. Също така бихме желали да изразим нашата благодарност на службата на Европейския надзорен орган за защита на данните за предоставената обратна връзка по време на изготвянето на материала. Особено сме благодарни на отдела за

защита на данните към Европейската комисия за помощта по време на писането на този наръчник.

Накрая, бихме желали да изразим нашата благодарност на Комисията за защита на личните данни, която прегледа превода на Ръководството на български език.

Philippe Boillat

Генерален директор по правата на човека и върховенството на закона на Съвета на Европа Съдържание

Morten Kjaerum

Директор на Агенцията на Европейския съюз за основните права

Съдържание

Съкращения и акроними

BCR	Задължителни корпоративни правила
CCTV	Вътрешна система за видеонаблюдение
CETS	Поредица договори на Съвета на Европа
CRM	Управление на връзките с клиенти
ENISA	Агенция на Европейския съюз за мрежова и информационна сигурност
ESMA	Европейски орган за ценни книжа и пазари
eTEN	Трансевропейски телекомуникационни мрежи
eu-LISA	Агенция на ЕС за широкомащабни информационни системи
EuroPriSe	Европейски печат за неприкосновеност на личния живот
FRA	Агенция на Европейския съюз за основните права
GPS	Глобална система за определяне на местоположението
PIN	Персонален идентификационен номер
PNR данни	Резервационни данни на пътниците
SEPA	Единна зона за плащания в евро
SWIFT	Дружество за световни междубанкови финансови телекомуникации
ВДПЧ	Всеобща декларация за правата на човека
ВИС	Визова информационна система
ДЕС	Договор за Европейския съюз
ДФЕС	Договор за функциониране на Европейския съюз
ЕАСТ	Европейска асоциация за свободна търговия
ЕЗА	Европейска заповед за арест
ЕО	Европейска общност

ЕКПЧ	Европейска конвенция за защита на правата на човека и основните свободи
ЕС	Европейски съюз
ЕНОЗД	Европейски надзорен орган по защита на данните
ЕИП	Европейско икономическо пространство
ЕСПЧ	Европейски съд по правата на човека
Конвенция № 108	Конвенция (на Съвета на Европа) за защита на лицата при автоматизираната обработка на лични данни
МИС	Митническа информационна система
НЗЕ	Национално звено на ЕВРОПОЛ
НПО	Неправителствена организация
Н-ШИС	Национална Шенгенска информационна система
ОИСР	Организация за икономическо сътрудничество и развитие
ООН	Организация на обединените нации
СЕ	Съвет на Европа
СНО	Съвместен надзорен орган
Съд на ЕС	Съд на Европейския съюз (преди декември 2009 г. наричан Съд на Европейските общности — СЕО)
Хартата	Харта на основните права на Европейския съюз
Ц-ШИС	Централна Шенгенска информационна система
ШИС	Шенгенска информационна система

Как да се използва този наръчник

В наръчника се съдържа преглед на приложимото право в областта на защитата на данните, свързано с Европейския съюз (ЕС) и Съвета на Европа (СЕ).

Наръчникът е предназначен да помага на практикуващите юристи, които не са специализирани в областта на защитата на данните; той е предназначен за адвокати, съдии или други практикуващи юристи, както и за работещите за други органи, включително неправителствени организации (НПО), които могат да се сблъскат с правни въпроси, свързани със защитата на данните.

Наръчникът е първа отправна точка за справки в областта на защитата на данните, както по отношение на правото на ЕС, така и на Европейската конвенция за правата на човека (ЕСПЧ), и в него се обяснява как тази област е уредена в правото на ЕС и в ЕКПЧ, както и в Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108), и в други инструменти на Съвета на Европа. Във всяка глава най-напред е дадена единна таблица на приложимите правни разпоредби, включително важна избрана съдебна практика в рамките на двете отделни европейски правни системи. След това съответните закони на тези две европейски уредби са представени един след друг, в зависимост от приложимостта им спрямо всяка тема. Това позволява на читателя да види в кои области двете правни системи се сближават и в кои се различават.

В таблиците в началото на всяка глава се изброяват разглежданите в нея теми и поименно се посочват приложимите правни разпоредби и други подходящи материали, като например съдебна практика. Подреждането на темите може леко да се различава от структурата на текста в рамките на дадената глава, ако това е счетено за по-удобно за краткото представяне на съдържанието на главата. Таблиците обхващат както правото на Съвета на Европа, така и правото на ЕС. Това би следвало да помогне на ползващите наръчника да намерят основната информация, отнасяща се до тяхното положение, особено ако спрямо тях се прилага само правото на Съвета на Европа.

Практикуващите юристи в държави извън ЕС, които са държави членки на Съвета на Европа, и страни по ЕКПЧ и Конвенция № 108 могат да имат достъп до информацията, приложима за тяхната собствена държава, като отидат направо на разделите относно Съвета на Европа. Практикуващите юристи в държавите членки на ЕС, ще трябва да използват и двата раздела, тъй като тези държави са обвързани и с двете правни уредби. За тези, които се нуждаят от повече информация по конкретен въпрос, списък с препратки към

по-специализирани материали може да бъде намерен в раздела „Допълнителна литература“ на наръчника.

Правото на Съвета на Европа е представено чрез кратки препратки към избрани дела на Европейски съд по правата на човека (ЕСПЧ). Те са избрани сред големия брой присъди и решения на ЕСПЧ, които съществуват по въпроси, свързани със защитата на данните.

Правото на ЕС се изразява в законодателни мерки, които са приети в съответните разпоредби на Договорите и в Хартата на основните права на Европейския съюз съгласно тълкуването в съдебната практика на Съда на Европейския съюз (Съд на ЕС, в други текстове наричан преди 2009 г. Съд на Европейските общности (СЕО)).

Съдебната практика, описана или цитирана в настоящия наръчник, представя примери за важна част от съдебната практика на ЕСПЧ, както и на Съда на ЕС. Насоките в края на наръчника са предназначени да помогнат на читателя в търсенето на съдебна практика онлайн.

В допълнение, в текстови карета са представени практически примери с хипотетични сценарии, за да се илюстрира на практика, прилагането на европейските правила за защита на данните, по-специално, когато по темата не съществува конкретна съдебна практика на ЕСПЧ или на Съда на ЕС.

Наръчникът започва с кратко описание на ролята на двете правни системи, както са определени от ЕКПЧ и правото на ЕС (глава 1). Глави 2—8 обхващат следните въпроси:

- терминологията в областта на защитата на данните;
- основните принципи на европейското право в областта на защитата на данните;
- правилата на европейското право в областта на защитата на данните;
- правата на съответните физически лица и тяхното прилагане;
- трансграничните потоци от данни;
- защитата на данните в контекста на полицията и наказателното правосъдие;
- други специални европейски закони за защита на данните.

1

Контекст и предистория на европейското право в областта на защитата на данните

ЕС	Обхванати въпроси	Съвет на Европа
Правото на защита на данните		
Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (*Директива за защита на личните данни*), ОВ L 281, 23.11.1995 г.		ЕКПЧ, член 8 (право на зачитане на личния и семейния живот, на жилището и тайната на кореспонденцията) Конвенция за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108)
Балансиране на правата		
Съд на ЕС, Решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR u Hartmut Eifert /Land Hessen*, C-92/09 и C-93/09	**Общо по въпросите**	
Съд на ЕС, Решение от 16 декември 2008 г. по дело *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy u Satamedia Oy*, C-73/07	**Свобода на изразяване на мнение**	ЕСПЧ, Решение от 2012 г. по дело *Axel Springer AG/Германия* ЕСПЧ, Решение от 2011 г. по дело *Mosley/Обединеното кралство*
	Свобода на изкуствата и науките	ЕСПЧ, Решение от 2007 г. по дело *Vereinigung bildender Künstler/Австрия*
Съд на ЕС, Решение от 29 януари 2008 г. по дело *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06	**Защита на собствеността**	
Съд на ЕС, Решение от 29 юни 2010 г. по дело *Европейска комисия/The Bavarian Lager Co. Ltd*, C-28/08 P	**Достъп до документи**	ЕСПЧ, Решение от 2009 г. по дело *Társaság a Szabadságjogokért/Унгария*

1.1. Правото на защита на данните

Ключови въпроси

- Съгласно член 8 от ЕКПЧ правото на защита срещу събирането и използването на лични данни е част от правото на зачитане на личния и семейния живот, на жилището и тайната на кореспонденцията.
- Конвенция № 108 на Съвета на Европа е първият международен правнообвързващ инструмент, в който изрично се разглежда защитата на данните.
- В рамките на правото на ЕС защитата на данните е уредена за първи път в Директивата за защита на личните данни.
- Съгласно правото на ЕС защитата на данните е призната като основно право.

Правото на защита на личния живот на лицето срещу намеса от страна на другите, особено от страна на държавата, беше предвидено в международен правен акт за първи път в член 12 от Всеобщата декларация на ООН за правата на човека (ВДПЧ) от 1948 г. относно зачитането на личния и семейния живот[1]. ВДПЧ оказа влияние върху разработването на други актове относно правата на човека в Европа.

1.1.1. Европейската конвенция за защита на правата на човека и основните свободи

Съветът на Европа беше създаден след края на Втората световна война, за да обедини европейските държави с цел насърчаване на върховенството на закона, демокрацията, правата на човека и социалното развитие. За тази цел, през 1950 г., той прие Европейската конвенция за защита на правата на човека и основните свободи (ЕСПЧ), която влезе в сила през 1953 г.

Държавите са поели международно задължение да спазват ЕКПЧ. Всички държави членки на Съвета на Европа, вече са включили или са привели в действие ЕКПЧ в своето национално законодателство, което изисква от тях да действат в съответствие с разпоредбите на Конвенцията.

За да се гарантира, че договарящите се страни спазват задълженията си съгласно ЕКПЧ, през 1959 г. беше създаден Европейският съд по правата на

1 Организация на обединените нации (ООН), Всеобща декларация за правата на човека (ВДПЧ), 10 декември 1948 г.

човека (ЕСПЧ) в Страсбург, Франция. ЕСПЧ гарантира, че държавите спазват своите задължения съгласно Конвенцията, като разглежда жалби от лица, групи лица, неправителствени организации или юридически лица относно предполагаеми нарушения на Конвенцията. През 2013 г. Съветът на Европа включваше 47 държави членки, 28 от които са също и държави членки на ЕС. Не е необходимо жалбоподателят пред ЕСПЧ да бъде гражданин на някоя от държавите членки. ЕСПЧ може също така да разглежда междудържавни дела, заведени от една или повече държави членки на Съвета на Европа, срещу друга държава членка.

Правото на защита на личните данни е част от правата, защитени съгласно член 8 от ЕКПЧ, който гарантира правото на зачитане на личния и семейния живот, на жилището и кореспонденцията и определя условията, при които се допускат ограничения на това право[2].

В своята съдебна практика ЕСПЧ е разгледал много ситуации, в които е възникнал въпросът за защита на данните, и не на последно място тези, свързани с прихващането на комуникации[3], различните форми на наблюдение[4] и защитата срещу съхраняването на лични данни от публичните органи[5]. Той е разяснил, че член 8 от ЕКПЧ не само задължава държавите да се въздържат от всякакви действия, които биха могли да нарушат това, предвидено в Конвенцията право, но и че при определени обстоятелства те имат и положителни задължения активно да гарантират ефективното зачитане на личния и семейния живот[6]. Много от тези дела ще бъдат разгледани подробно в съответните глави.

2 Съвет на Европа, Европейска конвенция за защита на правата на човека и основните свободи, CETS № 005, 1950 г.

3 Вж. например ЕСПЧ, Решение от 2 август 1984 г. по дело *Malone/Обединеното кралство*, № 8691/79; ЕСПЧ, Решение от 3 април 2007 г. по дело *Copland/Обединеното кралство*, № 62617/00.

4 Вж. например ЕСПЧ, Решение от 6 септември 1978 г. по дело *Klass и други/Германия*, № 5029/71, ЕСПЧ, Решение от 2 септември 2010 г. по дело *Uzun/Германия*, № 35623/05.

5 Вж. например ЕСПЧ, Решение от 26 март 1987 г. по дело *Leander/Швеция*, № 9248/81; ЕСПЧ, Решение от 4 декември 2008 г. по дело *S. и Marper/Обединеното кралство*, Nos. 30562/04 and 30566/0.

6 Вж. например ЕСПЧ, Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03, ЕСПЧ, Решение от 2 декември 2008 г. по дело *K.U/Финландия*, № 2872/02.

1.1.2. Конвенция № 108 на Съвета на Европа

С появата на информационните технологии през 60-те години на XX в. възникна нарастваща необходимост от по-подробни правила за защита на физическите лица чрез защита на техните (лични) данни. До средата на 70-те години на XX в., Комитетът на министрите на Съвета на Европа прие различни резолюции относно защитата на личните данни, позовавайки се на член 8 от ЕКПЧ[7]. През 1981 г. беше открита за подписване Конвенция за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108)[8]. Конвенция № 108 беше и все още продължава да бъде единственият правнообвързващ международен инструмент в областта на защитата на данните.

Конвенция 108 се прилага за цялостната обработка на данни, извършена в частния и публичния сектор, като обработката на данни от съдебни и правоприлагащи органи. Тя защитава лицето срещу злоупотреби, които могат да съпровождат събирането и обработването на личните данни, и едновременно с това има за цел да уреди трансграничното предоставяне на лични данни. По отношение на събирането и обработването на лични данни установените в конвенцията принципи се отнасят по-специално до добросъвестното и законосъобразното събиране и автоматично обработване на данни, съхранявани за определени законни цели, а не за да се използват за други несъвместими с тях цели, нито да се съхраняват за по-дълъг срок, отколкото е необходимо. Тези принципи също така се отнасят до качеството на данните, по-специално до това, че данните трябва да бъдат достатъчни, релевантни, точни и да не бъдат прекомерни спрямо целта (принципа за пропорционалност).

В допълнение към предоставянето на гаранции по отношение на събирането и обработването на лични данни, конвенцията забранява, при липсата на подходящи правни гаранции, обработването на „чувствителни" данни, като например данни относно расата, политическите възгледи, здравословното

7 Съвет на Европа, Комитет на министрите (1973 г.), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector [*Резолюция (73) 22 относно защитата на неприкосновеността на личния живот на лицата по отношение на електронните бази от данни в частния сектор*], 26 септември 1973 г.; Съвет на Европа, Комитет на министрите (1974 г.), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector [*Резолюция (74) 29 относно защитата на неприкосновеността на личния живот на лицата по отношение на електронните бази от данни в публичния сектор*], 20 септември 1974 г.

8 СЕ, Конвенция за защита на лицата при автоматизираната обработка на лични данни, Съвет на Европа, CETS № 108, 1981 г.

състояние, религията, сексуалния живот или съдебното досие на дадено лице.

Конвенцията също така утвърждава правото на лицето да бъде осведомено, че за него се съхранява информация и ,при необходимост, да поиска нейното коригиране. Ограниченията на правата, предвидени в конвенцията, са възможни само когато са застрашени първостепенни интереси като например държавната сигурност или отбраната.

Въпреки че конвенцията гарантира свободния обмен на лични данни между държавите — страни по нея, тя налага някои ограничения върху движението на тези данни към държави, в които правната уредба не предоставя равностойна защита.

С цел по-нататъшно развиване на общите принципи и правила, установени в Конвенция № 108, Комитетът на министрите на Съвета на Европа прие няколко препоръки, които нямат правнообвързващ характер (вж. глави 7 и 8).

Всички държави членки на ЕС са ратифицирали Конвенция № 108. През 1999 г. Конвенция № 108 беше изменена, за да може ЕС да стане страна по нея[9]. През 2001 г. беше приет Допълнителен протокол към Конвенция № 108, с който бяха въведени разпоредби относно трансграничните потоци от данни към държави, които не са страни по конвенцията, така наречените трети държави, както и относно задължителното създаване на национални надзорни органи за защита на данните[10].

Перспективи

След решение за осъвременяване на Конвенция № 108, чрез обществена консултация, проведена през 2011 г., стана възможно да бъдат потвърдени двете основни цели на този документ: засилването на защитата на неприкосновеността на личния живот в дигиталното пространство и укрепването на предвидения в конвенцията, механизъм за последващи действия.

9 Съвет на Европа, Изменения на Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), позволяващи на Европейските общности да се присъединят към нея, приети от Комитета на министрите в Страсбург на 15 юни 1999 г.; член 23, параграф 2 от Конвенция 108 в нейния изменен вид.

10 Съвет на Европа, Допълнителен протокол относно контролните органи и трансграничните потоци от данни към Конвенцията за защита на лицата при автоматизираната обработка на лични данни, CETS № 181, 2001 г.

Конвенция № 108 е отворена за присъединяване на държави, които не са членки на Съвета на Европа, включително и за неевропейски държави. Потенциалът на Конвенцията като универсален стандарт и нейният отворен характер биха могли да послужат като основа за насърчаване на защитата на данните в световен мащаб.

Досега 45 от 46-те договарящи се страни по Конвенция № 108 са държави членки на Съвета на Европа. Уругвай, първата неевропейска държава, се присъедини през август 2013 г., а Мароко, която беше поканена да се присъедини към Конвенция 108 от Комитета на министрите, е в процес на официално оформяне на присъединяването.

1.1.3. Право на Европейския съюз в областта на защитата на данните

Правото на ЕС се състои от договорите и вторичното право на ЕС. Договорите, а именно Договорът за Европейския съюз (ДЕС) и Договорът за функционирането на Европейския съюз (ДФЕС), са одобрени от всички държави членки на ЕС, и се наричат също „първично право на ЕС". Регламентите, директивите и решенията на ЕС са приети от институциите на ЕС, на които са били предоставени такива правомощия съгласно договорите; те често се наричат „вторично право на ЕС".

Основният правен инструмент на ЕС за защита на данните е Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни *(Директивата за защита на личните данни)*[11]. Тя бе приета през 1995 г. по време, когато няколко държави членки вече бяха приели национални закони за защита на данните. Свободното движение на стоки, капитали, услуги и хора в рамките на вътрешния пазар изискваше наличието на свободно движение на данни, което можеше да бъде осъществено само ако държавите членки можеха да разчитат на еднакво високо ниво на защита на данните.

Тъй като целта на приемането на Директивата за защита на личните данни беше хармонизирането[12] на правото за защита на данните на национално

11 Директива за защита на личните данни, ОВ L 281, 23.11.1995 г., стр. 31.

12 Вж. например Директивата за защита на личните данни, съображения 1, 4, 7 и 8.

равнище, директивата позволява известна степен на специфичност, съпоставима с тази на (тогава) съществуващите национални закони за защита на данните. Според СЕС, „Директива 95/46/ЕО е създадена с цел [....] гарантиране, че нивото на защита на правата и свободите на лицата по отношение на обработката на личните им данни е еквивалентна във всички страни членки. [....] Сближаването на приложимите национални законодателства в тази област не трябва да доведе до отслабване на защитата, която те предоставят, а обратно, да се стреми към осигуряването на високо ниво на защита в ЕС. Съответно [....] хармонизацията на тези национални законодателства не се ограничава до минимално изискваната, а до възможно най-всеобхватната“[13]. В резултат на това,държавите членки имат само ограничена свобода на действие при прилагането на директивата. Директивата за защита на личните данни е предназначена да придаде съдържание на принципите на правото на неприкосновеност на личния живот, които вече се съдържат в Конвенция № 108, както и да ги разшири. Фактът, че всички 15 държави членки на ЕС, през 1995 г. са били също и договарящи се страни по Конвенция № 108, изключва възможността за приемането на противоречиви правила в тези два правни инструмента. Директивата за защита на личните данни обаче се основава на възможността, предвидена в член 11 от Конвенция № 108, за добавяне на инструменти за защита. По-специално въвеждането на независимия надзор като инструмент за подобряване на съответствието с правилата за защита на данните се оказа важен принос за ефективното функциониране на европейското право в областта на защитата на данните. (Впоследствие чрез Допълнителния протокол към Конвенция 108 през 2001 г. тази функция бе включена в правото на Съвета на Европа).

Териториалното прилагане на Директивата за защита на личните данни се простира отвъд 28-те държави членки на ЕС, включително и в държавите, които не са членки на ЕС, но са част от Европейското икономическо пространство (ЕИП)[14], а именно Исландия, Лихтенщайн и Норвегия.

СЕСв Люксембург е компетентен да определя дали дадена държава членка е изпълнила своите задължения съгласно Директивата за защита на личните данни и да дава преюдициални заключения относно валидността, и

13 СЕС, Съвместни казуси C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) u Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 ноември 2011, ал. 28-29.

14 Споразумението за Европейското икономическо пространство, ОВ L 1, 3.1.1994 г., което влезе в сила на 1 януари 1994 г.

тълкуването на директивата, за да се гарантира нейното ефективно и еднакво прилагане в държавите членки. Важно изключение във връзка с прилагането на Директивата за защита на личните данни е т.нар. изключение за домашни дейности, а именно обработването на лични данни от физически лица само за „лични или домашни нужди“[15].Това обработване обикновено се разглежда като част от свободите на съответното физическо лице.

В съответствие с първичното право на ЕС, което е било в сила по време на приемането на Директивата за защита на личните данни, материалният обхват на директивата е ограничен до въпроси, свързани с вътрешния пазар. Най-важните въпроси, останали извън нейното приложно поле, са въпросите, свързани с полицейското сътрудничество и сътрудничеството в областта на наказателното правосъдие. Защитата на данните, свързана с тези въпроси, произтича от различни правни инструменти, които са описани подробно в глава 7.

Тъй като Директивата за защита на личните данни би могла да бъде адресирана само до държавите членки на ЕС, бе необходим допълнителен правен инструмент, за да се въведе защита на данните при обработването на лични данни от институциите и органите на ЕС. Регламент (ЕО) № 45/2001 относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни *(Регламент относно защитата на данните при обработването им от институции на ЕС)* изпълнява тази задача[16].

Освен това, дори и в области, обхванати от Директивата за защита на личните данни, често са необходими по-подробни разпоредби за защита на данните, за да се постигне необходимата яснота по отношение на балансирането на другите законни интереси. Два примера за това са Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (*Директива за правото на неприкосновеност на личния живот и*

15 Директива за защита на личните данни, член 3, параграф 2, второ тире.

16 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г.

електронни комуникации)[17] и Директива 2006/24/ЕО за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (*Директива за запазване на лични данни,произнесена за невалидна на 08 април 2014 г.*)[18]. Други примери ще бъдат обсъдени в глава 8. Тези разпоредби трябва да бъдат в съответствие с Директивата за защита на личните данни.

Хартата на основните права на Европейския съюз

Първоначалните договори на Европейските общности не съдържаха никакво посочване на правата на човека или на тяхната защита. Когато обаче в тогавашния Съд на Европейските общности (СЕО) бяха заведени дела за предполагаеми нарушения на правата на човека в области, попадащи в обхвата на правото на ЕС, Съдът разработи нов подход. За да предостави защита на физическите лица, той включи основните права в така наречените общи принципи на европейското право. Съгласно Съда на Европейския съюз тези общи принципи отразяват съдържанието на защитата на правата на човека, установена в националните конституции и договорите за правата на човека, по-специално в ЕКПЧ. Съдът на ЕС заяви, че ще гарантира съответствието на правото на ЕС с тези принципи.

Признавайки, че неговите политики биха могли да окажат въздействие върху правата на човека и за да се чувстват гражданите по-свързани с ЕС, през 2000 г., ЕС провъзгласи Хартата на основните права на Европейския съюз (Хартата). Тази харта включва целия спектър от граждански, политически, икономически и социални права на европейските граждани, като излага в синтезиран вид общите за държавите членки конституционни традиции и международни задължения. Правата, описани в Хартата, са групирани в шест раздела: „Достойнство“, „Свободи“, „Равенство“, „Солидарност“, „Права на гражданите“ и „Правосъдие“.

17 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (*Директива за правото на неприкосновеност на личния живот и електронни комуникации*), ОВ L 201, 31.7.2002 г.

18 Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, *(Директива за запазване на лични данни)*, ОВ L 105, 13.4.2006 г., произнесена за невалидна на 08 април 2014 г.

Въпреки че първоначално бе само политически документ, с влизането в сила на Договора от Лисабон на 1 декември 2009 г., Хартата придоби правнообвързващ характер[19] като първично право на ЕС (вж. член 6, параграф 1 от Договора за Европейския съюз)[20].

Първичното право на ЕС също така съдържа обща компетентност на ЕС да приема законодателни актове по въпроси, свързани със защитата на данните (член 16 от ДФЕС).

Хартата не само гарантира зачитането на личния и семейния живот (член 7), но също така установява правото на защита на личните данни (член 8), като изрично издига нивото на тази защита в правото на ЕС до това на основно право. Институциите на ЕС, както и държавите членки, трябва да спазват и да гарантират това право, което се отнася и за държавите членки, когато те прилагат правото на Съюза (член 51 от Хартата). Формулиран няколко години след приемането на Директивата за защита на личните данни, член 8 от Хартата трябва да се тълкува като израз на съществуващото преди това право на ЕС в областта на защитата на данните. Поради това в Хартата не само изрично се указва правото на защита на данните в член 8, параграф 1, но също така се посочват основните принципи за защита на данните в член 8, параграф 2. Накрая, в член 8, параграф 3 от Хартата се гарантира, че прилагането на тези принципи ще подлежи на контрол от независим орган.

Перспективи

През януари 2012 г. Европейската комисия предложи пакет от реформи за защита на данните, като заяви, че настоящите правила за защита на данните е необходимо да бъдат модернизирани с оглед на бързото развитие на технологиите и глобализацията. Пакетът от реформи се състои от предложение за общ регламент относно защитата на данните[21], предназначен да замени Директивата за защита на личните данни, както и от нова директива за

19 ЕС (2012 г.), Харта на основните права на Европейския съюз, ОВ C 326, 26.10.2012 г.

20 Вж. Европейски общности (2012 г.), Консолидирани текстове на Договора за Европейския съюз, ОВ C 326, 26.10.2012 г. и на Договора за функционирането на Европейския съюз, ОВ C 326, 26.10.2012 г.

21 Европейска комисия (2012 г.), *Предложение за регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (общ регламент относно защитата на данните*), COM(2012) 011 окончателен, Брюксел, 25 януари 2012 г.

защита на личните данни[22], която да предвижда защита на данните в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси. Към момента на публикуването на настоящия наръчник течеше обсъждане на пакета от реформи.

1.2. Балансиране на правата

Ключов въпрос

- Правото на защита на данните не е абсолютно право, то трябва да бъдат балансирано спрямо другите права.

Основното право на защита на личните данни съгласно член 8 от Хартата „не е абсолютно право, а трябва да се разглежда по отношение на неговата функция в обществото“[23]. Поради това в член 52, параграф 1 от Хартата се приема, че могат да бъдат налагани ограничения относно упражняването на правата като например на правата, определени в членове 7 и 8 от Хартата, доколкото такива ограничения са предвидени по закон, зачитат същността на тези права и свободи, и при спазване на принципа за пропорционалност, са необходими, и действително отговарят на признати от Европейския съюз цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора[24].

В системата на ЕКПЧ защитата на данните е гарантирана в член 8 (право на зачитане на личния и семейния живот) и, както и в системата на Хартата, това право трябва да се прилага при зачитане на обхвата на прилагане на другите конкуриращи се права. Съгласно член 8, параграф 2 от ЕКПЧ „намесата на държавните власти в ползването на това право е недопустима освен в случаите,

22 Европейска комисия (2012 г.), *Предложение за директива на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни(обща директива за защита на личните данни)*, COM(2012) 010 окончателен, Брюксел, 25 януари 2012 г.

23 Вж. например Съд на ЕС, Решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR и Hartmut Eifert Land Hessen*, съединени дела C-92/09 и C-93/09, точка 48.

24 *Пак там*, точка 50.

предвидени в закона и необходими в едно демократично общество [...] за защита [...] на правата и свободите на другите".

Вследствие на това както ЕСПЧ, така и Съдът на ЕС многократно са заявявали, че при прилагането и тълкуването на член 8 от ЕКПЧ и член 8 от Хартата е необходимо постигането на баланс спрямо другите права[25]. Няколко важни примера ще илюстрират как се постига този баланс.

1.2.1. Свобода на изразяване на мнение

Едно от правата, които е възможно да влязат в противоречие с правото на защита на данните, е правото на свобода на изразяване на мнение.

Свободата на изразяване на мнение е защитена в член 11 от Хартата („Свобода на изразяване на мнение и свобода на информация"). Това право включва „свободата да отстоява своето мнение, да получава и да разпространява информация и идеи без намеса на държавните власти, и независимо от границите". Член 11 съответства на член 10 от ЕКПЧ. Съгласно член 52, параграф 3 от Хартата, доколкото тя съдържа права, съответстващи на правата, гарантирани от ЕКПЧ, „техният смисъл и обхват са същите като дадените им в посочената Конвенция". Ограниченията, които могат да бъдат законно наложени на правото, гарантирано в член 11 от Хартата, следователно не могат да превишават предвидените в член 10, параграф 2 от ЕКПЧ, т.е. те трябва да са предвидени от закона и да са необходими в едно демократично общество „за защитата [...] на репутацията или правата на другите". Тази концепция обхваща правото на защита на данните.

Съотношението между защитата на личните данни и свободата на изразяване на мнение се урежда в член 9 от Директивата за защита на личните данни, озаглавен „Обработка на личните данни и свобода на изразяване"[26]. Съгласно

25 ЕСПЧ, Решение от 7 февруари 2012 г. по дело *Von Hannover/Германия (№ 2)* [голям състав], № 40660/08 и 60641/08; Съд на ЕС, Решение от 24 ноември 2011 г. по съединени дела *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) и Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, съединени дела C-468/10 и C-469/10, точка 48; Съд на ЕС, Решение от 29 януари 2008 г. по дело *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06 68. Вж. също Съвет на Европа (2013 г.), Съдебна практика на Европейския съд по правата на човека относно защитата на личните данни, Защита на данните (2013 г.) — съдебна практика, достъпни на адрес: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP%202013%20Case%20Law_Eng%20%28final%2018%2007%202013%29.pdf.

26 Директива за защита на личните данни, член 9.

този член-„държавите членки са задължени да предвиждат редица дерогации или ограничения по отношение на „обработването на лични данни“ и следователно, и по отношение на основното право на неприкосновеност на личния живот, посочени в глави II, IV и VI от директивата. Тези дерогации трябва да се извършват „единствено за целите на журналистическа дейност или на литературно или художествено изразяване“, които попадат в обхвата на основното право на свобода на изразяване на мнение „само ако са необходими за съгласуването на правото на личен живот с правилата, регулиращи свободата на изразяване“.

Пример: В дело *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy u Satamedia Oy*[27] от Съда на ЕС бе поискано да даде тълкуване на член 9 от Директивата за защита на личните данни и да определи съотношението между защитата на личните данни и свободата на изразяване. Съдът трябваше да разгледа разпространяването от страна на Markkinapörssi и Satamedia на данъчни данни за приблизително 1,2 милиона физически лица, законно получени от финландските данъчни органи. По-специално, Съдът трябваше да провери дали обработването на предоставени от данъчните органи лични данни, с цел да се даде възможност на потребителите на мобилни телефони да получават данъчни данни, отнасящи се до други физически лица, трябва да се разглежда като дейност, извършвана единствено за целите на журналистическата дейност. След като стигна до заключението, че извършените от Satakunnan дейности представляват „обработване на лични данни“ по смисъла на член 3, параграф 1 от Директивата за защита на личните данни, Съдът продължи с тълкуване на член 9 от директивата. На първо място Съдът отбеляза значението на правото на свобода на изразяване на мнение във всяко демократично общество и постанови, че понятия, свързани с тази свобода, като журналистиката, следва да бъде предмет на широко тълкуване. След това той отбеляза, че с цел постигане на баланс между двете основни права дерогациите и ограниченията на правото на защита на данните трябва да се прилагат само дотолкова, доколкото това е строго необходимо. При тези обстоятелства Съдът счете, че дейности като тези, извършени от Markkinapörssi и Satamedia, отнасящи се до данни от документи, които са обществено достояние съгласно националното законодателство, могат да бъдат класифицирани като „журналистически

27 Съд на ЕС, Решение от 16 декември 2008 г. по дело *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy u Satamedia Oy*, C-73/07, точки 56, 61 и 62.

дейности“, ако тяхната цел е разкриване пред обществеността на информация, мнения или идеи, независимо от използвания носител за тяхното предаване. Съдът постанови също, че тези дейности не са ограничени до медийни дейности и могат да бъдат предприети с търговска цел. Съдът на ЕС обаче остави на националния съд да определи дали в това конкретно дело случаят е такъв.

Що се отнася до съвместяването на правото на защита на данните с правото на свобода на изразяване на мнение, ЕСПЧ е издал няколко принципни решения.

Пример: По делото *Axel Springer AG/Германия*[28] ЕСПЧ е постановил, че забраната, наложена от национален съд на собственик на вестник, който искал да публикува статия за арестуването и осъждането на известен актьор, е в нарушение на член 10 от ЕСПЧ. ЕСПЧ отново е посочил критериите, установени от него в съдебната му практика при балансирането на правото на свобода на изразяване и правото на зачитане на личния живот:

- първо, дали въпросното публикуване на статията е било въпрос от обществен интерес: арестуването и осъждането на лице е било публичен съдебен факт и следователно предизвиква обществен интерес;
- второ, дали съответното лице е публична личност: въпросното лице е било достатъчно известен актьор, за да бъде квалифицирано като публична личност; и
- трето, как е получена информацията и дали е била надеждна: информацията е била предоставена от прокуратурата и достоверността ѝ в двете публикации не е била оспорена от страните.

Поради това ЕСПЧ е постановил, че ограниченията за публикуване, наложени на дружеството, не са били пропорционални на преследваната законна цел за защита на личния живот на жалбоподателя. Съдът е заключил, че е налице нарушение на член 10 от ЕКПЧ.

28 ЕСПЧ, Решение от 7 февруари 2012 г. по дело *Axel Springer AG/Германия* [голям състав], № 39954/08, точки 90 и 91.

Пример: По делото *Von Hannover/Германия (№ 2)*[29] ЕСПЧ не е установил нарушение на правото на зачитане на личния живот съгласно член 8 от ЕКПЧ, когато на принцесата на Монако — Каролин, е отказано да предяви иск срещу публикуването на нейна и на съпруга ѝ снимка, направена по време на ски ваканция. Снимката е била придружена от статия, в която, наред с други въпроси, се съобщава за лошото здравословно състояние на принц Рение. ЕСПЧ е заключил, че националните съдилища внимателно са балансирали правото на свободата на изразяване на мнение на издателските дружества спрямо правото на зачитане на личния живот на жалбоподателите. Направеното от националните съдилища характеризиране на заболяването на принц Рение като събитие за съвременното общество не може да се счита за необосновано и ЕСПЧ е могъл да приеме, че снимката, която е била разгледана във връзка със статията, най-малкото до известна степен допринася за повдигането на дебат от обществен интерес. Съдът е заключил, че не е налице нарушение на член 8 от ЕКПЧ.

В съдебната практика на ЕСПЧ един от най-важните критерии по отношение балансирането на тези права е дали изразяването по даден въпрос допринася за дебат от обществен интерес.

Пример: В делото *Mosley/Обединеното кралство*[30] национален седмичник е публикувал снимки на жалбоподателя от интимно естество. Тогава той е заявил, че член 8 от ЕКПЧ е бил нарушен, тъй като не е можел да предяви иск преди публикуването на въпросните снимки поради липсата на изискване за предварително известяване от вестника в случай на публикуване на материал, нарушаващ правото на неприкосновеност на личния живот. Въпреки че разпространението на такъв материал е било по-скоро с развлекателна, отколкото с образователна цел, то несъмнено се ползва от защитата, предвидена в член 10 от ЕКПЧ, което може да отстъпи пред изискванията на член 8 от ЕКПЧ в случаите, в които информацията е била от частно и интимно естество и нейното разпространение не е било от обществен интерес. Въпреки това е трябвало да се обърне особено внимание при разглеждането на ограниченията, които биха

29 ЕСПЧ, Решение от 7 февруари 2012 г. по дело *Von Hannover/Германия (№ 2)* [голям състав], № 40660/08 и 60641/08, точки 118 и 124.

30 ЕСПЧ, Решение от 10 май 2011 г. по дело *Mosley/Обединеното кралство*, № 48009/08, точки 129 и 130.

могли да имат функцията на форма на цензура преди публикуването. Що се отнася до възпиращия ефект, до който може да доведе изискването за предварително известяване, до съмненията за ефективността му и до голямата свобода на преценка в тази област, ЕСПЧ е заключил, че съгласно член 8 не е необходимо наличието на изискване за правнообвързващо предварително известяване. Поради това Съдът е заключил, че не е налице нарушение на член 8.

Пример: По делото *Biriuk/Литва*[31] жалбоподателката е предявила иск за нанесени щети от ежедневен вестник, тъй като е публикувал статия, в която се твърди, че тя е ХИВ позитивна. Съществуват твърдения, че тази информация е била потвърдена от медици от местната болница. ЕСПЧ не е счел, че въпросната статия допринася за какъвто и да е дебат от общ интерес и отново е заявил, че защитата на личните данни, не на последно място на медицинските данни, е от особена важност, за да може лицето да се ползва от правото си на зачитане на личния и семейния живот, както е гарантирано в член 8 от ЕКПЧ. Съдът е придал особена важност на факта, че съгласно репортажа в статията, медицинският персонал в болницата е предоставил информация относно ХИВ заболяването на жалбоподателката, което е явно нарушение на тяхното задължение да пазят медицинска тайна. Следователно държавата не е гарантирала правото на жалбоподателката на зачитане на личния ѝ живот. Съдът е заключил, че е налице нарушение на член 8.

1.2.2. Достъп до документи

Свободата на информацията съгласно член 11 от Хартата и член 10 от ЕКПЧ защитава правото не само да се съобщава, но също и да се *получава* информация. Наблюдава се все-по голямо осъзнаване на значението на прозрачността на управлението за функционирането на едно демократично общество. Вследствие на това през последните две десетилетия правото на достъп до документи, съхранявани от публичните органи, беше признато като основно право на всеки гражданин на ЕС, както и на всяко физическо или юридическо лице, което пребивава или е със седалище в държава членка.

Съгласно правото на Съвета на Европа може да се прави позоваване на принципите, установени в Препоръката относно достъпа до официални документи,

31 ЕСПЧ, Решение от 25 ноември 2008 г. по дело *Biriuk/Литва*, № 23373/03.

която е вдъхновила създателите на Конвенцията относно достъпа до официални документи (*Конвенция 205*)[32]. **Съгласно правото на ЕС** правото на достъп до документи е гарантирано в Регламент (ЕО) № 1049/2001 относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията (*Регламент относно достъпа до документи*)[33]. Член 42 от Хартата и член 15, параграф 3 от ДФЕС разшириха това право на достъп „до документите на институциите, органите, службите и агенциите на Съюза, независимо от вида на техния носител". В съответствие с член 52, параграф 2 от Хартата, правото на достъп до документи се упражнява също така при условията и в границите, предвидени в член 15, параграф 3 от ДФЕС. Това право може да влезе в противоречие с правото на защита на данните, в случай че достъпът до даден документ би разкрил лични данни на други лица. Поради това, по отношение на исканията за достъп до документи или данни, съхранявани от публичните органи, може да е необходимо балансиране на правото на защита на личните данни на лицата, чиито данни се съдържат в исканите документи.

Пример: В делото *Комисия/Bavarian Lager*[34] Съдът на ЕС определи обхвата на защитата на лични данни в контекста на достъпа до документи на институциите на ЕС и връзката между Регламент (ЕО) № 1049/2001 (*Регламента относно достъпа до документи*) и Регламент (ЕО) № 45/2001 (*Регламента относно защитата на данните*). Bavarian Lager, учредено през 1992 г., внася бутилирана немска бира в Обединеното кралство, предимно за кръчми и барове. То обаче е срещнало трудности, тъй като британското законодателство *де факто* е облагодетелствало националните производители. В отговор на жалбата на Bavarian Lager Европейската комисия е решила да заведе дело срещу Обединеното кралство за неизпълнение на неговите задължения, което е довело до това то да изменени спорните разпоредби и да ги приведе в съответствие с правото на ЕС. След това Bavarian Lager е поискало от Комисията, наред с други документи, копие от протокола от събрание, на което

32 Съвет на Европа, Комитет на министрите (2002 г.), Препоръка Rec(2002)2 до държавите членки относно достъпа до официални документи, 21 февруари 2002 г., Съвет на Европа, Конвенция относно достъпа до официални документи, CETS № 205, 18 юни 2009 г. Конвенцията все още не е влязла в сила.

33 Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 г. относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията, ОВ L 145, 31.05.2001 г.

34 Съд на ЕС, Решение от 29 юни 2010 г. по дело *Европейска комисия/The Bavarian Lager Co. Ltd*, C-28/08 P, точки 60, 63, 76, 78 и 79.

са присъствали представители на Комисията, на британските органи и *Confédération des Brasseurs du Marché Commun* (CBMC). Комисията се е съгласила да оповести някои документи във връзка със събранието, но е заличила пет имена в протокола, тъй като две лица изрично са се противопоставили на оповестяването на тяхната самоличност, а с другите три Комисията не е успяла да установи контакт. С решение от 18 март 2004 г. Комисията е отхвърлила новото искане на Bavarian Lager за получаване на пълния протокол от събранието, позовавайки се по-специално на защитата на личния живот на тези лица, както е гарантирана в Директивата за защита на данните. Тъй като не е удовлетворено от тази позиция, Bavarian Lager подава жалба до Първоинстанционния съд, който отменя решението на Комисията с решение от 8 ноември 2007 г. (дело *Bavarian Lager/Комисия*, T-194/04), като по-специално счита, че самото вписване на имената на въпросните лица в списъка на лицата, присъствали на събрание, от името на органа, който те представляват, не представлява накърняване на неприкосновеността на техния личен живот и не застрашава личния живот на тези лица.

При обжалване от страна на Комисията, Съдът на ЕС е отменил решението на Първоинстанционния съд. Съдът на ЕС е постановил, че Регламентът относно достъпа до документи установява „специфичен засилен режим на защита на лице, чиито лични данни евентуално биха могли да бъдат предоставени на обществеността“. Според Съда на ЕС в случаите, когато чрез искане, основано на Регламента относно достъпа до документи, се цели получаването на достъп до документи, включително лични данни, разпоредбите на Директиватаза защита на данните стават приложими в тяхната цялост. След това Съдът на ЕС заключи, че Комисията е имала право да отхвърли заявлението за достъп до пълния протокол от събранието от октомври 1996 г. При липсата на съгласието на петимата участници в това събрание Комисията, в достатъчна степен, е спазила задължението си за откритост, като е оповестила версия на въпросния документ, в която техните имена са заличени.

Освен това според Съда на ЕС „тъй като Bavarian Lager не е предоставило никаква изрична и легитимна обосновка, нито убедителен довод, за да докаже необходимостта от предаване на тези лични данни, Комисията не е могла да прецени различните интереси на съответните страни. Тя не е могла и да провери дали няма основания да се предполага, че това

предаване би могло да засегне легитимните интереси на субектите на данните“, както се изисква от Директивата за защитат на данните.

Съгласно това решение е необходима конкретна и основателна причина за намеса в правото на защита на данните във връзка с достъпа до документи. Правото на достъп до документи не може автоматично да отменя правото на защита на данните[35].

Конкретен аспект на искането за достъп е разгледан в следното решение на ЕСПЧ.

Пример: В дело *Társaság a Szabadságjogokért/Унгария*[36] жалбоподателят, НПО по правата на човека, е поискала от Конституционния съд достъп до информация относно висящо дело. Без да се консултира с члена на парламента, който е завел делото пред него, Конституционният съд е отхвърлил искането за достъп на основание, че подадените до него жалби могат да се оповестяват на външни лица само със съгласието на тъжителя. Националните съдилища са потвърдили този отказ на основание, че други законни интереси, включително достъпността до публична информация, не могат да имат преимущество пред защитата на такива лични данни. Жалбоподателят е действал като „обществен пазител“, чиито дейности се ползват с подобна защита като защитата, предоставяна на печата. По отношение на свободата на печата, ЕСПЧ многократно е постановявал, че обществото има право да получава информация от общ интерес. Исканата от жалбоподателя информация е била „налична и на разположение“ и не е изисквала никакво събиране на данни. При тези обстоятелства държавата е имала задължение да не възпрепятства предоставянето на исканите от жалбоподателя данни. Казано накратко, ЕСПЧ е счел, че пречките, предназначени да възпрепятстват достъпа до информация от обществен интерес, могат да обезсърчат работещите в медиите или свързаните с нея области да изпълняват своята жизненоважна роля на „обществен страж“. Съдът е заключил, че е налице нарушение на член 10.

35 Вж. обаче подробните обсъждания на Европейския надзорен орган по защита на данните (ЕНОЗД) (2011 г.), *Публичен достъп до съдържащи лични данни документи след решението по делото Bavarian Lager*, Брюксел, 24 март 2011 г., достъпни на адрес: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 ЕСПЧ, Решение от 14 април 2009 г. по дело *Társaság a Szabadságjogokért/Унгария*, № 37374/05; вж. точки 27, 36—38.

Съгласно правото на ЕС значението на прозрачността е ясно определено. Принципът за прозрачност е установен в членове 1 и 10 от ДЕС и в член 15, параграф 1 от ДФЕС[37]. Съгласно съображение 2 от Регламент (ЕО) № 1049/2001 този принцип дава възможност на гражданите да участват в процеса на вземане на решения и е гаранция за по-голяма законност, ефективност и отговорност на администрацията по отношение на гражданите в демократичната система[38].

Следвайки тази логика, Регламент (ЕО) № 1290/2005 на Съвета относно финансирането на Общата селскостопанска политика и Регламент (ЕО) № 259/2008 на Комисията за установяване на подробни правила за прилагане на Регламент (ЕО) № 1290/2005 изискват публикуването на информация относно бенефициентите по определени фондове на ЕС в сектора на селското стопанство и относно сумите, получени от всеки бенефициент[39]. Публикуването следва да допринесе за обществения контрол върху правилното използване на публични средства от страна на администрацията. Пропорционалността на това публикуване беше оспорена от няколко бенефициенти.

Пример: В делото *Volker und Markus Schecke u Hartmut Eifert/Land Hessen*[40] Съдът на ЕС трябваше да прецени пропорционалността на изискването, съгласно законодателството на ЕС, публикуване на имената на бенефициентите на селскостопански субсидии от ЕС и на получените от тях суми.

Съдът, като отбеляза, че правото на защита на данните не е абсолютно право, заяви, че публикуването в уеб сайт на поименни данни относно бенефициентите по двата фонда на ЕС за селскостопански помощи и

37 ЕС (2012 г.), Консолидирани текстове на Договора за Европейския съюз и на Договора за функционирането на Европейския съюз, ОВ C 326, 26.10.2012 г.

38 Съд на ЕС, Решение от 6 март 2003 г. по дело *Interporc Im- und Export GmbH/Комисия на Европейските общности*, C-41/00 P, точка 39; и Съд на ЕС, Решение от 29 юни 2010 г. по дело *Европейска комисия/The Bavarian Lager Co. Ltd*, C-28/08 P, точка 54.

39 Регламент (ЕО) № 1290/2005 на Съвета от 21 юни 2005 г. относно финансирането на Общата селскостопанска политика, ОВ L 209, 11.8.2005 г.; и Регламент (ЕО) № 259/2008 на Комисията от 18 март 2008 г. за установяване на подробни правила за прилагане на Регламент (ЕО) № 1290/2005 относно публикуването на информация за получателите на средства от Европейския фонд за гарантиране на земеделието (ЕФГЗ) и Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР), ОВ L 76, 19.3.2008 г.

40 Съд на ЕС, Решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR (C-92/09) u Hartmut Eifert (C-93/09)/Land Hessen*, съединени дела C-92/09 и C-93/09, точки 47—52, 58, 66—67, 75, 86 и 92.

точните размери на получените от тях суми представлява намеса в личния им живот като цяло, и по-специално в защитата на техните лични данни.

Съдът счете, че тази намеса по отношение на членове 7 и 8 от Хартата е предвидена от закона и изпълнява призната от ЕС цел от общ интерес, включително и целта за повишаване на прозрачността на използването на общностни фондове. Съдът на ЕС обаче постанови, че публикуването на имената на физическите лица — бенефициенти на селскостопанска помощ от ЕС, по линия на тези два фонда, както и на точните размери на получените от тях суми представлява непропорционална мярка и не е обосновано от гледна точка на член 52, параграф 1 от Хартата. По този начин, Съдът обяви за частично недействително законодателството на ЕС относно публикуването на информация, свързана с бенефициентите по европейски земеделски фондове.

1.2.3. Свобода на изкуствата и науките

Друго право, което трябва да бъде балансирано спрямо правото на неприкосновеност на личния живот и правото на защита на данните, е свободата на изкуствата и науките, изрично защитена съгласно член 13 от Хартата. Това право произтича основно от свободата на мисълта и на изразяване на мнение и трябва да се упражнява, като се взема предвид член 1 от Хартата („Човешко достойнство"). ЕСПЧ счита, че свободата на изкуствата е защитена съгласно член 10 от ЕКПЧ[41]. Правото, гарантирано в член 13 от Хартата, може също така да подлежи на ограниченията, разрешени в член 10 от ЕКПЧ[42].

Пример: В дело *Vereinigung bildender Kunstler/Австрия*[43] австрийските съдилища са забранили на сдружението жалбоподател да продължи да излага на показ картина, която съдържа фотоизображения на главите на редица публични личности в сексуални пози. Австрийски парламентарист, чиято снимка е била използвана в картината, е предявил иск срещу сдружението жалбоподател, като е поискал съдебна възбрана срещу показването на картината. Националният съд е издал забрана, приемайки

41 ЕСПЧ, Решение от 24 май 1998 г. по дело *Müller и други/Швейцария*, № 10737/84.

42 Разяснения относно Хартата на основните права, ОВ C 303, 14.12.2007 г.

43 ЕСПЧ, Решение от 25 януари 2007 г. по дело *Vereinigung bildender Künstler/Австрия*, № 68345/01; вж. по-специално точки 26 и 34.

неговото искане. ЕСПЧ отново е заявил, че член 10 от ЕКПЧ е приложим по отношение на разпространяването на идеи, които обиждат, шокират или смущават държавата или определена част от населението. Лицата, които създават, представят, разпространяват или показват произведения на изкуството, допринасят за обмена на идеи и мнения и държавата има задължението да не накърнява неправомерно свободата им на изразяване. Като се има предвид, че картината е колаж и са използвани само фотоизображения на главите на лицата и че телата им са изобразени по нереалистичен и преувеличен начин, който очевидно не цели да отразява или дори да загатва реалността, ЕСПЧ заяви още, че „картината едва ли би могла да се разбира като представяща подробности от личния живот на [изобразеното лице], а по-скоро е свързана с неговото обществено положение като политик“ и че „в това си качество [изобразеното лице] е трябвало да прояви по-голяма толерантност по отношение на критиките“. Претегляйки различните изложени на опасност интереси, ЕСПЧ установи, че неограничената възбрана на по-нататъшното показване на картината е непропорционална. Съдът е заключил, че е налице нарушение на член 10 от ЕКПЧ.

Що се отнася до науката, европейското право в областта на защитата на данните осъзнава специалното значение на науката за обществото. Поради това общите ограничения за използването на лични данни са намалени. Както Директивата за защита на личните данни, така и Конвенция № 108 разрешават запазването на данни за целите на научни изследвания, след като тези данни вече не са необходими за първоначалната цел, за която са били събрани. Освен това последващото използване на лични данни за целите на научни изследвания не се счита за несъвместима цел. Националното законодателство е натоварено със задачата за изготвянето на по-подробни разпоредби, включително и на необходимите гаранции, за съвместяване на интересите във връзка с научните изследвания с правото на защита на данните (вж. също раздели 3.3.3 и 8.4).

1.2.4. Защита на собствеността

Правото на защита на собствеността е установено в член 1 от Първия протокол към ЕКПЧ, както и в член 17, параграф 1 от Хартата. Един важен аспект на правото на собственост е защитата на интелектуалната собственост, изрично посочена в член 17, параграф 2 от Хартата. В правния ред на ЕС могат да бъдат намерени няколко директиви, които имат за цел ефективна защита

на интелектуалната собственост, и по-специално на авторското право. Интелектуалната собственост обхваща не само литературната и художествената собственост, но и патентите, търговските марки, и сродните права.

Както ясно показва съдебната практика на Съда на ЕС, защитата на основното право на собственост трябва да бъде балансирана спрямо защитата на други основни права, по-специално спрямо правото на защитата на данните[44]. Има дела, в които институции за защита на авторското право са поискали от интернет доставчиците да разкрият самоличността на потребителите на интернет платформи за споделяне на файлове. Такива платформи често правят възможно за интернет потребителите да изтеглят безплатно музикални произведения, въпреки че тези произведения са защитени с авторско право.

Пример: Делото *Promusicae/Telefónica de España*[45] се отнася до отказа на испански доставчик на услуги за достъп до интернет, Telefónica, да разкрие на Promusicae, организация с нестопанска цел, в която членуват музикални продуценти и издатели на музикални и аудиовизуални звукозаписи, личните данни на определени лица, на които то е предоставяло услуги за достъп до интернет. Promusicae е поискало разкриването на тази информация, за да може да предяви граждански искове срещу тези лица, за които твърди, че използват програма за споделяне на файлове, която им осигурява достъп до звукозаписи, чиито права на ползване се притежават от членовете на Promusicae.

Испанският съд е отнесъл въпроса до Съда на ЕС, като е отправил запитване дали такива лични данни трябва да бъдат оповестени съгласно общностното право в рамките на гражданско производство, за да се осигури ефективната защита на авторското право. Той се е позовал на Директиви 2000/31, 2001/29 и 2004/48, тълкувани също в контекста на членове 17 и 47 от Хартата. Съдът заключи, че тези три директиви, както и Директивата за правото на неприкосновеност на личния живот и електронни комуникации (Директива 2002/58/ЕО) не изключват възможността държавите членки да предвидят задължение за разкриване на лични данни в рамките на гражданско производство, за да осигурят ефективна защита на авторското право.

44 ЕСПЧ, Решение от 10 януари 2013 г. по дело *Ashby Donald и други/Франция*, № 36769/08.

45 Съд на ЕС, Решение от 29 януари 2008 г. по дело *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06, точки 54 и 60.

Съдът на ЕС посочи, че следователно делото повдига въпроса за необходимостта от съвместяване на изискванията за защита на различните основни права, а именно на правото на зачитане на личния живот с правото на защита на собствеността и правото на ефективни средства за правна защита.

Съдът заключи, че „при транспониране на посочените по-горе директиви държавите членки трябва да следят за тълкуване на последните, което позволява да се осигури подходящо равновесие между различните основни права, защитени от общностния правов ред. На следващо място, при въвеждане на мерките за транспониране на тези директиви, органите и юрисдикциите на държавите членки са длъжни не само да тълкуват националното си право по начин, който да съответства на посочените директиви, но и да не допускат да се основават на тълкуване, което би влязло в конфликт с посочените основни права или с другите общи принципи на общностното право като принципа на пропорционалност“[46].

46 *Пак там*, точки 65 и 68; вж. също Съд на ЕС, Решение от 16 февруари 2012 г по дело *SABAM/Netlog N.V,* C-360/10.

2

Терминология в областта на защитата на данните

ЕС	Обхванати въпроси	Съвет на Европа
Лични данни		
Директива за защита на личните данни, член 2, буква а) Съд на ЕС, Решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR (C-92/09) u Hartmut Eifert (C-93/09)/Land Hessen*, съединени дела C-92/09 и C-93/09 Съд на ЕС, Решение от 29 януари 2008 г. по дело *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06	**Правно определение**	Конвенция № 108, член 2, буква а) ЕСПЧ, Решение от 14 март 2013 г. по дело *Bernh Larsen Holding AS и други/Норвегия*, № 24117/08
Директива за защита на личните данни, член 8, параграф 1 Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01	**Специални категории лични данни (чувствителни данни)**	Конвенция № 108, член 6
Директива за защита на личните данни, член 6, параграф 1, буква д)	**Анонимизирани данни и данни под псевдоним**	Конвенция № 108, член 5, буква д) Конвенция № 108, Обяснителен доклад, член 42
Обработване на данни		
Директива за защита на личните данни, член 2, буква б) Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01	**Определения**	Конвенция № 108, член 2, буква в)

Ползватели на данни		
Директива за защита на личните данни, член 2, буква г)	**Администратор**	Конвенция № 108, член 2, буква г) Препоръка относно профилирането, член 1, буква ж) *
Директива за защита на личните данни, член 2, буква д) Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01	**Обработващ**	Препоръка относно профилирането, член 1, буква з)
Директива за защита на личните данни, член 2, буква ж)	**Получател**	Конвенция № 108, Допълнителен протокол, член 2, параграф 1.
Директива за защита на личните данни, член 2, буква е)	**Трето лице**	
Съгласие		
Директива за защита на личните данни, член 2, буква з) Съд на ЕС, Решение от 5 май 2011 г. по дело *Deutsche Telekom AG/ Bundesrepublik Deutschland*, C-543/09	**Определение и изисквания за валидно съгласие**	Препоръка относно медицинските данни, член 6, както и различни последващи препоръки

Забележка: **Съвет на Европа, Комитет на министрите (2010 г.), Препоръка Rec(2010)13 до държавите членки относно защитата на лицата при автоматизираната обработка на лични данни в контекста на профилиране (Препоръка относно профилирането), 23 ноември 2010 г.*

2.1. Лични данни

Ключови въпроси

- Данните са лични данни, ако те се отнасят до идентифицирано лице или поне до подлежащо на идентификация лице — съответното физическо лице, което е субект на данните.
- Едно лице е подлежащо на идентификация, ако без прекомерни усилия може да бъде получена допълнителна информация, позволяваща идентифицирането на съответното физическо лице.Автентификация означава доказване, че дадено лице притежава определена самоличност и/или е получило разрешение за извършването на определени дейности.
- Има специални категории данни, така наречените чувствителни данни, посочени в Конвенция № 108 и в Директивата за защита на личните данни, които

се нуждаят от засилена защита и поради това са обект на специален правен режим.

- Данните са анонимизирани, ако вече не съдържат никакви идентификатори;Те са псевдонимизирани , ако идентификаторите са в криптирана форма.
- За разлика от анонимизираните данни,псевдонимизираните данни са лични данни.

2.1.1. Основни аспекти на понятието „лични данни“

Съгласно правото на ЕС, както и **правото на Съвета на Европа,** „личните данни“ се определят като информация, свързана с идентифицирано или подлежащо на идентификация лице[47], т.е. информация за лице, чиято самоличност е напълно изяснена или най-малкото може да бъде установена чрез получаване на допълнителна информация.

Ако данните на такова лице се обработват, това лице се нарича „субект на данни“.

Лице

Правото на защита на данните произтича от правото на неприкосновеност на личния живот. Понятието „личен живот“ се отнася за човешките същества. Следователно физическите лица са основните бенефициенти на защитата на данните. Освен това съгласно Становището на Работната група за защита на личните данни по член 29 (Работната група по член 29) само *„живите личности“* са защитени съгласно европейското право за защита на данните[48].

Съдебната практика на ЕСПЧ по отношение на член 8 от ЕКПЧ показва, че е трудно напълно да се разделят въпросите, свързани с личния живот, от тези, свързани с професионалния живот[49].

47 Директива за защита на личните данни, член 2, буква а); Конвенция № 108, член 2, буква а).

48 Работна група за защита на личните данни по член 29 (2007 г.), *Становище № 4/2007 относно понятието „лични данни“*, WP 136, 20 юни 2007 г., стр. 22.

49 Вж. например ЕСПЧ, Решение от 4 май 2000 г. по дело *Rotaru/Румъния* [голям състав], № 28341/95, точка 43; ЕСПЧ, Решение от 16 декември 1992 г. по дело *Niemitz/Германия*, № 13710/88, точка 29.

Пример: В делото *Amann/Швейцария*[50] органите са прихванали делови телефонен разговор до жалбоподателя. Въз основа на това обаждане, органите са разследвали жалбоподателя и са попълнили карта за него в картотеката на службата за национална сигурност. Въпреки че прихващането се е отнасяло до делови телефонен разговор, ЕСПЧ е счел, че съхраняването на данни относно това обаждане има връзка с личния живот на жалбоподателя. Съдът е посочил, че терминът „личен живот" не трябва да се тълкува ограничително, по-специално тъй като неприкосновеността на личния живот обхваща правото на създаване и поддържане на отношения с други човешки същества. Освен това не е било налице принципно основание, с което да се оправдае изключването на дейности от професионално или бизнес естество от понятието „личен живот". Такова широко тълкуване е отговаряло на това от Конвенция № 108. ЕСПЧ освен това е установил, че в случая на жалбоподателя намесата не е била в съответствие със закона, тъй като националното законодателство не е съдържало специални и подробни разпоредби относно събирането, записването и съхраняването на информация. Поради това Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

Освен това, ако въпросите, свързани с професионалния живот, могат също да подлежат на защита на данните, изглежда спорно дали единствено за данните на физически лица следва да се предоставя защита. Правата съгласно ЕКПЧ са гарантирани не само за физическите лица, а за всички.

Съществува съдебна практика на ЕСПЧ от произнесени решения по жалби на юридически лица, свързани с предполагаемо нарушение на правото им на защита по отношение на използването на техните данни съгласно член 8 от ЕКПЧ. Съдът обаче е разгледал случая съгласно правото на неприкосновеност на жилището и кореспонденцията, а не на правото на неприкосновеностна личния живот.

Пример: Делото *Bernh Larsen Holding AS и други/Норвегия*[51] се е отнасяло до жалба от три норвежки дружества относно решение на данъчните

50 ЕСПЧ, Решение от 16 февруари 2000 г. по дело *Amann/Швейцария* [голям състав], № 27798/95, точка 65.

51 ЕСПЧ, Решение от 14 март 2013 г. по дело *Bernh Larsen Holding AS и други/Норвегия*, № 24117/08. Вж. обаче и ЕСПЧ, Решение от 1 юли 2008 г. по дело *Liberty и други/Обединеното кралство*, № 58243/00.

органи, по силата на което от тях се изисква да предоставят на данъчните одитори копие на всички данни от компютърния сървър, който трите дружества са използвали съвместно.

ЕСПЧ е установил, че такова задължение на дружествата жалбоподатели представлява намеса в правото им на неприкосновеност на „жилището" и „кореспонденцията" за целите на член 8 от ЕКПЧ. Съдът обаче е счел, че данъчните органи са имали ефективни и адекватни гаранции срещу злоупотреба: дружествата жалбоподатели са били уведомени предварително; те са присъствали и са били в състояние да изложат своите доводи по време на намесата на място; материалът е трябвало да бъде унищожен след приключването на данъчната ревизия. При тези обстоятелства е бил осигурен подходящ баланс между правото на дружествата жалбоподатели на неприкосновеност на „жилището" и „кореспонденцията" и техния интерес да защитят неприкосновеността на личния живот на хората, работещи за тях, от една страна, и обществения интерес по отношение на осигуряването на ефективна инспекция за целите на проверката за установяване на данъчни задължения, от друга страна. Съдът е постановил, че поради тази причина не е налице нарушение на член 8.

Съгласно Конвенция № 108 защитата на данните се свързва основно със защитата на физически лица; въпреки това договарящите се страни могат да разширят обхвата на защитата на данните и до юридически лица, като например дружества и асоциации, които попадат в обхвата на националното им законодателство. **Правото на ЕС в областта на защитата на данните,** като цяло, не включва защитата на юридически лица, що се отнася до обработването на свързани с тях данни. Националните регулаторни органи имат свободата да уредят този въпрос[52].

Пример: В делото *Volker und Markus Schecke GbR/Land Hessen*[53] Съдът на ЕС, позовавайки се на публикуването на лични данни за бенефициентите на селскостопански помощи е постановил, че „юридическите лица могат да се позоват на защитата по членове 7 и 8 от Хартата по отношение на подобно идентифициране само доколкото в наименованието на юридическото лице се идентифицират едно или повече физически лица. [...]

52 Директива за защита на личните данни, съображение 24.

53 Съд на ЕС, Решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR (C-92/09) u Hartmut Eifert (C-93/09)/Land Hessen*, съединени дела C-92/09 и C-93/09, точка 53.

Зачитането на правото на личен живот с оглед на обработката на лични данни, признато с членове 7 и 8 от Хартата, се отнася до всяка информация относно идентифицирано или подлежащо на идентификация физическо лице [...]“[54].

Идентифицируемост на дадено лице

Съгласно правото на ЕС, както и **това на Съвета на Европа,** в определена информация се съдържат данни за дадено лице, ако:

- лицето е идентифицирано в тази информация; или
- ако дадено лице, въпреки че не е идентифицирано, е описано в тази информация по такъв начин, че е възможно да се открие за кое физическо лице става въпрос при продължаване на проучването.

И двата вида информация са защитени по един и същ начин от европейското право в областта на защитата на данните. ЕСПЧ многократно е заявявал, че понятието „лични данни“ по смисъла на ЕКПЧ е същото като и в Конвенция № 108, особено що се отнася до условието за информация относно идентифицирани или подлежащи на идентификация лица[55].

Правните определения за личните данни не изясняват допълнително кога дадено лице се счита за идентифицирано[56]. Очевидно идентификацията изисква елементи, които описват лицето по такъв начин, че то се различава от всички останали и се разпознава като физическо лице. Името на даден човек е основен пример за такива елементи на описание. В някои изключителни случаи, други определения могат да имат подобен ефект като този на името. Например, по отношение на публичните личности може да е достатъчно да се спомене длъжността на лицето, например председател на Европейската комисия.

54 *Пак там,* точка 52.

55 Вж. ЕСПЧ, Решение от 16 февруари 2000 г. по дело *Amann/Швейцария* [голям състав], № 27798/95, точка 65 и др.

56 Вж. също ЕСПЧ, Решение от 13 февруари 2003 г. по дело *Odièvre/Франция* [голям състав], № 42326/98; и ЕСПЧ, Решение от 25 септември 2012 г. по дело *Godelli/Италия*, № 33783/09.

Пример: В решението по дело *Promusicae*[57] Съдът на ЕС е постановил, че „не се оспорва, че поисканото от Promusicae съобщаване на имената и адресите на определени лица, ползващи „KaZaA“ [определена интернет платформа за споделяне на файлове], включва предоставяне на лични данни, т.е. на сведения относно точно идентифицирани или подлежащи на идентификация физически лица, съгласно определението в член 2, буква а) от Директива 95/46 [...]. Съобщаването на тези сведения, които според Promusicae са съхранявани от Telefónica, като последното не оспорва това обстоятелство, представлява обработка на лични данни по смисъла на член 2, първа алинея от Директива 2002/58 във връзка с член 2, буква б) от Директива 95/46.“

Тъй като много имена не са уникални, установяването на самоличността на дадено лице може да изисква допълнителни идентификатори, за да се докаже, че лицето не е сбъркано с някой друг. Често се използват датата и мястото на раждане. В допълнение, в някои държави са въведени персонализирани номера за по-добро разпознаване на гражданите. Биометричните данни като дактилоскопични отпечатъци, цифрови снимки или сканиране на ириса придобиват все по-голямо значение за идентификацията на лица в технологичната ера.

За приложимостта на европейското право в областта на защитата на данните обаче не е необходима висококачествена идентификация на физическото лице, достатъчно е въпросното лице да бъде идентифицирано. Дадено лице се счита за идентифицируемо, ако част от информацията съдържа елементи на идентификация, чрез които лицето може да бъде идентифицирано пряко или непряко[58]. Съгласно съображение 26 от Директивата за защита на личните данни критерият е дали е вероятно, че разумни средства за идентификация ще бъдат на разположение и ще бъдат администрирани от предвидените ползватели на данните; това включва и получателите — трети лица (вж. раздел 2.3.2).

Пример: Местен орган решава да събира данни за автомобили, движещи се с превишена скорост по местните улици. Колите се заснемат, като автоматично се записват времето и мястото, за да се предоставят данните на

57 Съд на ЕС, Решение от 29 януари 2008 г. по дело *Productores de Música de España (Promusicae)/ Telefónica de España SAU*, C-275/06, точка 45.

58 Директива за защита на личните данни, член 2, буква а).

компетентния орган, който съответно налага глоби на нарушителите на ограниченията на скоростта. Потърпевшо физическо лице подава жалба, твърдейки, че местният орган не разполага с правно основание съгласно законодателството за защита на данните да събира такива данни. Местният орган твърди, че не събира лични данни. Той заявява, че регистрационните номера представляват данни за анонимни лица. Местният орган не разполага с юридически правомощия за достъп до общия регистър на превозните средства, за да идентифицира собственика на автомобила или водача.

Тази логика не отговаря на съображение 26 от Директивата за защита на личните данни. Предвид факта, че целта на събирането на данни е ясно да се идентифицират водачите, които карат с превишена скорост и подлежат на глоба, е предвидимо, че ще се направи опит за идентификация. Въпреки че местните органи не разполагат пряко със средства за идентификация, те предават данните на компетентния орган, полицията, който разполага с такива средства. Съображение 26 също изрично включва сценарий, при който може да се предвиди, че следващите получатели на данни, които са различни от непосредствените ползватели на данните, могат да се опитат да идентифицират лицето. В контекста на съображение 26 действието на местния орган се равнява на събирането на данни за подлежащи на идентификация лица и следователно изисква законно основание съгласно правото зазащита на данните.

Съгласно правото на Съвета на Европа идентифицируемостта се разбира по подобен начин. Член 1, параграф 2 от Препоръката относно данните, използвани за платежни операции[59], например гласи, че едно лице не се счита за „подлежащо на идентификация“, ако разкриването на самоличността изисква неоправдан разход на време, средства или човешки ресурси.

Автентификация

Това е процедура, при която дадено лице може да докаже, че притежава определена самоличност и/или е оторизирано да извършва определени дейности, като влизане в зона за сигурност или теглене на пари от банкова сметка. Автентификацията може да се постигне чрез сравняване на

59 Съвет на Европа, Комитет на министрите (1990 г.), Препоръка № R Rec(90) 19 относно защитата на личните данни, използвани за платежни и други свързани с това операции, 13 септември 1990 г.

биометрични данни, като снимка или дактилоскопични отпечатъци в паспорт, с данните на лицето, представящо се за него, например, при имиграционен контрол; или чрез изискване на информация, която е известна само на лицето с определена самоличност или оторизация, като например личния идентификационен номер (PIN) или парола; или като се изисква представянето на определен знак или символ, който трябва да се притежава единствено от лице с определена идентичност или оторизация, например специална чип карта или ключ за банков сейф. Отделно от паролите или чип картите, понякога заедно с ПИН кодовете, електронните подписи са инструмент, който е особено подходящ за идентификация или автентификация на дадено лице при електронни комуникации.

Естество на данните

Всеки вид информация може да представлява лични данни, при условие че е тя е свързана с дадено лице.

> Пример: Оценката на ръководител за работата на служител, съхранявана в личното досие на служителя, представлява лични данни за него, въпреки че всъщност тази информация може просто да отразява, частично или изцяло, личното мнението на ръководителя, като например следното: „служителят не е отдаден на работата си“ и факти, които не са необорими, като: „работникът е отсъствал от работа пет седмици през последните шест месеца“.

Личните данни обхващат информация, която се отнася до личния живот на едно лице, както и информация относно неговия професионален или обществен живот.

В дело *Amann*[60] ЕСПЧ е дал тълкуване на термина „лични данни“ като понятие, което не се ограничава само до въпроси от сферата на личния живот на лицето (вж. раздел 2.1.1). Това значение на термина „лични данни“ се отнася също и до Директивата за защита на личните данни:

60 Вж. ЕСПЧ, Решение от 16 февруари 2000 г. по дело *Amann/Швейцария*, № 27798/95, точка 65.

Пример: В решението по дело *Volker und Markus Schecke u Hartmut Eifert/ Land Hessen*[61] Съдът на ЕС е постановил, че „в това отношение е без значение фактът, че публикуваните данни се отнасят до професионални дейности [...]. В тази връзка Европейският съд по правата на човека е приел относно тълкуването на член 8 от ЕКПЧ, че изразът „личен живот" не трябва да се тълкува ограничително и че „никакво принципно съображение не позволява да се изключат професионалните дейности [...] от понятието „личен живот".

Данните се отнасят за дадено лице, ако съдържанието на информацията косвено разкрива данни за лицето. В някои случаи, в които има тясна връзка между обект или събитие — напр. мобилен телефон, автомобил, инцидент, от една страна, и лицето — напр. като негов собственик, потребител, жертва — от друга страна, информацията за обекта или събитието също би трябвало да се счита за лични данни.

Пример: В дело *Uzun/Германия*[62] жалбоподателят и друг мъж били под наблюдение посредством устройство към Глобалната система за определяне на местоположението (GPS), поставено в автомобила на другия мъж, поради факта, че са били заподозрени за участие в бомбени атентати. В този случай ЕСПЧ е постановил, че наблюдението на жалбоподателя чрез GPS е равносилно на намеса в личния му живот, а това попада под защитата, определена в член 8 от ЕКПЧ. Въпреки това наблюдението посредством GPS е било в съответствие със закона, както и пропорционално на преследваната законна цел да бъдат разследвани няколко обвинения в опит за убийство и следователно е било необходимо в демократично общество. Съдът е постановил, че не е налице нарушение на член 8 от ЕКПЧ.

Форма на представяне на данните

Формата, под която се съхраняват или се използват личните данни, не е от значение при прилаганетона правото в областта на защитата на личните данни. Писмената и устната комуникация може да съдържа лични данни,

61 Решение от 9 ноември 2010 г. по съединени дела Volker und Markus Schecke GbR и Hartmut Eifert /Land Hessen, съединени дела C-92/09 и C-93/09, точка 59.

62 ЕСПЧ, Решение от 2 септември 2010 г. по дело *Uzun/Германия*, № 35623/05.

както и образи[63], включително кадри от системи за видеонаблюдение (CCTV)[64] или звук[65]. Електронно записваната информация, както и информацията на хартиен носител, може да представлява лични данни; дори клетките на човешката тъкан могат да бъдат лични данни, тъй като „записват" ДНК-то на лицето.

2.1.2. Специални категории лични данни

Съгласно правото на ЕС, както и **на Съвета на Европа,** има специални категории лични данни, които поради своето естество при тяхното обработване могат да представляват риск за физическите лица и се нуждаят от засилена защита. Следователно обработването на тези специални категории данни („чувствителни данни") трябва да бъде разрешено само при наличието на определени гаранции.

По отношение на определението за чувствителни данни, както в Конвенция № 108 (член 6), така и в Директивата за защита на личните данни (член 8) се посочват следните категории:

- лични данни, разкриващи расов или етнически произход;
- лични данни, разкриващи политически възгледи, религиозни или други убеждения; и
- лични данни, свързани със здравето или сексуалния живот.

Пример: В делото *Bodil Lindqvist*[66] Съдът на ЕС е посочил, че „споменаването на факта, че едно лице е наранило стъпалото си и по медицински съображения работи на половин работен ден, съставлява лични данни, засягащи здравето, по смисъла на член 8, параграф 1 от Директива 95/46/ЕО".

63 ЕСПЧ, Решение от 24 юни 2004 г. по дело *Von Hannover/Германия*, № 59320/00; ЕСПЧ, Решение от 11 януари 2005 г. по дело *Sciacca/Италия*, № 50774/99.

64 ЕСПЧ, Решение от 28 януари 2003 г. по дело *Peck/Обединеното кралство*, № 44647/98; ЕСПЧ, Решение от 5 октомври 2010 г. по дело *Köpke/Германия*, № 420/07.

65 Директива за защита на личните данни, съображения 16 и 17; ЕСПЧ, Решение от 25 септември 2001 г. по дело *P.G. и J.H./Обединеното кралство*, № 44787/98, точки 59 и 60; ЕСПЧ, Решение от 20 декември 2005 г. по дело *Wisse/Франция,* № 71611/01.

66 Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01, точка 51.

Освен това, в Директивата за защита на личните данни като чувствителни данни се посочва „членството в професионални съюзи“, тъй като тази информация може да бъде сериозен показател за политически убеждения или принадлежност.

Конвенция № 108 също разглежда личните данни, свързани с наказателни присъди, като чувствителни данни.

Член 8, параграф 7 от Директивата за защита на личните данни възлага на държавите членки да „определят условията, при които може да се обработва национален идентификационен номер или какъвто и да е друг идентификатор с общо приложение“.

2.1.3. Анонимизирани данни и псевдонимизирани данни

Според принципа за ограничен период на запазване на данните, съдържащ се в Директивата за защита на личните данни, както и в Конвенция № 108 (и обсъдени по-подробно в глава 3), данните трябва „да се поддържат във форма, която позволява идентифицирането на съответните физически лица за срок не по-дълъг от необходимия за целите, за които тези данни са събрани или обработени допълнително“[67]. Следователно данните би трябвало да бъдат анонимизирани, ако администраторът иска да ги съхранява, след като те вече не са актуални и вече не служат за тяхната първоначална цел.

Анонимизирани данни

Данните са анонимизирани, ако всички идентифицируеми елементи са били премахнати от определен набор лични данни. Никакъв елемент не може да бъде оставен в данните, който би могъл при полагането на разумни усилия да послужи за повторната идентификация на въпросното(ите) лице(а)[68]. Когато данните са анонимизирани успешно, те вече не са лични данни.

Ако личните данни вече не изпълняват първоначалната си цел, но се съхраняват в персонализирана форма с цел тяхното използване за исторически,

67 Директива за защита на личните данни, член 6, параграф 1, буква д); и Конвенция № 108, член 5, буква д).

68 *Пак там*, съображение 26.

статистически или научни цели, Директивата за защита на личните данни и Конвенция № 108 предвиждат такава възможност, при условие че са предоставени подходящи гаранции срещу злоупотреба[69].

Псевдонимизирани данни

Личните данни съдържат идентификатори като име, дата на раждане, пол и адрес. Когато личните данни са въведени под псевдоним, идентификаторите се заменят от един псевдоним. Представянето на данни чрез използването на псевдоним се постига, например, чрез криптиране на идентификаторите в личните данни.

Псевдонимизираните даннине са изрично упоменати в правните определения на Конвенция № 108 или на Директивата за защита на личните данни. В член 42 от Обяснителния доклад към Конвенция № 108 обаче се посочва, че „[изискването [...], което се отнася до времевите ограничения по отношение на съхраняването на данни под формата на инициали, не означава, че след известно време данните трябва да бъдат неотменимо отделени от името на лицето, за което се отнасят, а само че няма да е възможно да се направи лесна връзка между данните и идентификаторите“. Това е резултат, който може да бъде постигнат посредством представянето на данните чрез използване на псевдоним. За всеки, който не притежава ключа за декриптиране, псевдонимизираните данни могат да бъдат трудно идентифицирани; но връзката със самоличността все още съществува под формата на псевдоним плюс ключа за декриптиране. За тези, които имат право да използват ключа за декриптиране, е лесно да направят повторна идентификация. По-специално трябва да се предотврати използването на ключовете за криптиране от неупълномощени лица.

Тъй като представянето на данни чрез използване на псевдоним е едно от най-важните средства за осъществяване на защита на данните в голям мащаб, когато не е възможно пълно въздържане от използването на лични данни, логиката и резултатът от такова действие трябва да бъдат обяснени по-подробно.

69 *Пак там*, член 6, параграф 1, буква д); и Конвенция № 108, член 5, буква д).

Пример: Изречението „Чарлс Спенсър, роден на 3 април 1967 г., е баща на семейство с четири деца, две момчета и две момичета“ може например да бъде представено под следния псевдоним:

„Ч.С. 1967 г. е баща в семейство с четири деца, две момчета и две момичета“; или

„324 е баща в семейство с четири деца, две момчета и две момичета“; или

„YESz320l е баща в семейство с четири деца, две момчета и две момичета“.

Потребители, които имат достъп до тезипсевдонимизирани данни, обикновено не могат да идентифицират „Чарлс Спенсър, роден на 3 април 1967 г.“ чрез „324“ или „YESz3201“. Следователно въведените под псевдоним данни е по-вероятно да бъдат защитени от злоупотреба.

Първият пример, обаче, е по-малко сигурен. Ако изречението „Ч.С. 1967 г. е баща на семейство с четири деца, две момчета и две момичета“ се използва в едно малко село, където живее Чарлс Спенсър, г-н Спенсър може лесно да бъде разпознат. Методът на използване на псевдоним оказва влияние върху ефективността на защитата на данните.

Личните данни с криптирани идентификатори се използват в много различни контексти като средство за запазване на самоличността на лицата в тайна. Това е особено полезно в случаите, когато администраторите на данни трябва да гарантират, че работят със същите физически лица, но не изискват или не се нуждаят от истинската им самоличност. Такъв е случаят например, когато изследовател разучава хода на болестта при пациенти, чиято самоличност е известна само на болницата, в която са лекувани и от която изследователят получава епикризите на медицинските случаи с данни под псевдоним. Следователно използването на псевдоним е солиден инструмент в арсенала на технологиите за подобряване на неприкосновеността на личния живот. То може да функционира като важен елемент при осъществяване на защита на данните още при проектирането. Това означава включване на защитата на данните в напредналите системи за обработване на данни.

2.2. Обработване на данни

Ключови въпроси

- Терминът „обработване“ се отнася предимно до автоматизираното обработване.
- Съгласно правото на ЕС „обработването“ също така се отнася и до ръчното обработване в структурирани системи за обработване на данни по регистри.
- Съгласно правото на Съвета на Европа значението на термина „обработване“ може да бъде разширено от националното законодателство, така че да включва ръчното обработване.

Защитата на данни съгласно Конвенция № 108 и Директивата за защита на личните данни е съсредоточена основно върху автоматизираното обработване на данни.

Съгласно **правото на Съвета на Европа** в определението за автоматизирано обработване на данни обаче се отчита, че между отделните автоматизирани операции може да са необходими няколко етапа на ръчно използване на личните данни. По същия начин съгласно **правото на ЕС** автоматизираното обработване на данни се определя като „операции, прилагани спрямо личните данни, извършени изцяло или отчасти чрез автоматизирани средства“[70].

Пример: По делото *Bodil Lindqvist*[71] Съдът е постановил, че:

„операция, състояща се в обръщане, в интернет страница, към различни лица и определянето им или по име, или по друг начин, например чрез телефонен номер или данни, свързани с условията им на работа, и развлеченията им, представлява „пълна или частична обработка на лични данни с автоматизирани средства“ по смисъла на член 3, параграф 1 от Директива 95/46/ЕО“.

70 Конвенция № 108, член 2, буква в); и Директива за защита на личните данни, член 2, буква б) и член 3, параграф 1.

71 Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01, точка 27.

Ръчното обработване на данни също се нуждае от защита на данните.

Защитата на данните **съгласно правото на ЕС** по никакъв начин не се ограничава до автоматизирано обработване на данни. Съответно съгласно правото на ЕС защитата на данни се прилага спрямо обработването на лични данни в ръчна система за обработване на данни по регистри, която представлява, специално структурирано досие на хартиен носител[72]. Причината за това разширяване на обхвата на защитата на данните е следната:

- досиетата на хартиен носител могат да бъдат структурирани по начин, който прави намирането на информация бързо и лесно; и

- съхраняването на лични данни в структурирани досиета на хартиен носител прави лесно заобикалянето на ограниченията, предвидени от законодателството по отношение на автоматизираното обработване на данни[73].

Съгласно правото на Съвета на Европа, Конвенция № 108 урежда основно обработването на данни в автоматизирани регистри с данни[74]. Освен това, то предвижда възможността в обхвата на националното законодателство за защита на данните да бъде включено и ръчното обработване на данни Много страни по Конвенция № 108 са се възползвали от тази възможност, като за целта са подали декларации до генералния секретар на Съвета на Европа[75]. Разширяването на обхвата на защитата на данни съгласно тази декларация трябва да се отнася за всяко едно ръчно обработване на данни и не може да се ограничава до обработването в ръчни системи,съдържащи регистри[76].

Що се отнася до естеството на включените операции по обработване, понятието „обработване“ е изчерпателно определено, **както съгласно правото на ЕС, така и съгласно правото на Съвета на Европа**: „обработване на лични данни“ [...] означава всяка операция [...] като събиране, запис, организиране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друга форма на предоставяне на данните, актуализиране или комбиниране, блокиране, изтриване или

72 Директива за защита на личните данни, член 3, параграф 1.

73 *Пак там*, съображение 27.

74 Конвенция № 108, член 2, буква б).

75 Вж. декларациите, направени съгласно Конвенция № 108, член 3, параграф 2, буква в).

76 Вж. формулировката в Конвенция № 108, член 3, параграф 2.

унищожаване“[77], прилагана спрямо личните данни. Терминът „обработване“ включва също така дейности, при които данните излизат извън обхвата на отговорност на един администратор и се прехвърлят в рамките на отговорността на друг администратор.

Пример: Работодателите събират и обработват данни за своите служители, включително информация, свързана с техните заплати. Правното основание законно да правят това е трудовият договор.

Работодателите ще трябва да изпратят данните за заплатите на своите служители на данъчните органи. Това изпращане на данни също ще представлява „обработване“ по смисъла на този термин в Конвенция № 108 и в директивата. Правното основание за такова разкриване на данни обаче не е трудовият договор. Трябва да има допълнително правно основание за операциите по обработване, водещи до трансфера на данни за заплатите от работодателя на данъчните органи. Това правно основание обикновено се съдържа в разпоредбите на националното данъчно законодателство. Без такива разпоредби трансферът на данните би представлявал незаконно обработване.

2.3. Ползвателите на лични данни

Ключови въпроси

- Всяко лице, което реши да обработва лични данни на други лица, съгласно правото за защитата на данните е „администратор“; ако няколко лица взимат това решение заедно, те могат да бъдат „съвместни администратори“.
- „Обработващ “ означава лице със самостоятелна правосубектност, което обработва лични данни от името на администратора;
- Обработващият става администратор, ако използва данните за свои собствени цели, като не следва указанията на администратора.
- Всеки, който получава данни от администратор, е „получател“.

77 Директива за защита на личните данни, член 2, буква б). По същия начин вж. също Конвенция № 108, член 2, буква в).

- „Трето лице“ е физическо или юридическо лице, което не действа по нареждане на администратора (и не е физическото лице — субект на данните).
- „Получател — трето лице“ е лице или субект, който е юридически отделен от администратора, но получава лични данни от него.

2.3.1. Администратори и обработващи

Най-важната последица от това да се изпълнява ролята на администратор или на обработващ данни е правната отговорност за изпълнение на съответните задължения съгласно правото за защита на данните. Поради това, този статут се дава само на лица, които могат да бъдат подведени под отговорност съгласно приложимото право. В частния сектор обикновено това са физически или юридически лица; в публичния сектор това обикновено са органи. Други субекти, като органи или институции без правосубектност, могат да бъдат администратори или обработващи данни, само когато това е предвидено от специални правни разпоредби.

Пример: Когато отделът по маркетинг на дружеството Sunshine планира да обработва данни за пазарно проучване, администраторът на това обработване ще бъде самото дружество Sunshine, а не отделът по маркетинг. Отделът по маркетинг не може да бъде администратор, тъй като той не се ползва с отделен юридически статут.

В групите от дружества, дружеството майка и всяко дъщерно дружество, които са отделни юридически лица, се разглеждат като отделни администратори или обработващи данни лица. Като резултат от този отделен юридически статут трансферът на данни между дружествата, които членуват в група от компании, ще трябва да се извършва въз основа на специално правно основание. Липсва каквато и да било привилегия, свързана с разрешаване на обмена на лични данни между отделните правни субекти в рамките на групата от дружества.

В този контекст е необходимо да бъде посочена ролята на физическите лица. **Съгласно правото на ЕС,** физическите лица, когато обработват данни за други лица в хода на чисто лични или домашни занимания, не попадат в обхвата на разпоредбите на Директивата за защита на личните данни; те не се считат за администратори[78].

78 Директива за защита на личните данни, съображение 12 и член 3, параграф 2, последно тире.

От съдебната практика обаче става ясно, че въпреки товаправото на защита на данните е приложимо, когато лице публикува данни за други лица, докато използва интернет.

Пример: Съдът на ЕС е постановил по делото *Bodil Lindqvist*[79], че:

„операция, състояща се в обръщане, в интернет страница, към различни лица и определянето им или по име, или по друг начин, [...] представлява „пълна или частична обработка на лични данни с автоматизирани средства" по смисъла на член 3, параграф 1 от Директива 95/46/ЕО"[80].

Такова обработване на лични данни не попада в категорията на чисто личните или домашните дейности, които са извън обхвата на Директивата за защита на личните данни, тъй като това изключение „трябва [...] да се тълкува като отнасящо се само до дейности, които се извършват в хода на личния или семейния живот на физическите лица, какъвто очевидно не е случаят с обработването на лични данни, състоящо се в публикуването на тези данни в интернет, така че те да бъдат достъпни за неограничен брой хора"[81].

Администратор

Съгласно правото на ЕС администраторът е определен като субект, който „сам или съвместно с други определя целите и средствата на обработка на лични данни"[82]. С решение на администратора се определят причината за и начинът на обработване на данните. **Съгласно правото на Съвета на Европа** в определението за „администратор" също така се посочва, че администраторът решава кои категории лични данни следва да бъдат съхранявани[83].

В определението за администратор, съдържащо се в Конвенция № 108, се прави позоваване на другаспект от администрирането, който следва да бъде разгледан. В определението се прави препратка към въпроса, кой може законно да обработва определени данни за конкретна цел. Когато

79 Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01.

80 *Пак там*, точка 27.

81 *Пак там*, точка 47.

82 Директива за защита на личните данни, член 2, буква г).

83 Конвенция № 108, член 2, буква г).

обачесъществуват твърдения, че се извършват незаконни операции по обработване и трябва да бъде установен отговорният администратор, това ще бъде лицето или субектът, като дружество или орган, което е преценило, че данните следва да бъдат обработени, независимо от това дали - има законно право да извършва тази дейност или не[84]. По тази причина искането за изтриване на данни винаги трябва да бъде адресирано до „фактическия" администратор.

Съвместно обработване на лични данни от повече от един администратор

В определението за „администратор" в Директивата за защита на личните данни се предвижда, че може да има няколко лица със самостоятелна правосубектност, които заедно или съвместно с други лица действат като администратори. Това означава, че те решават заедно да обработват данни с определена обща цел[85]. Това е възможно от правна гледна точка, но само в случаите, в които въз основа на специално законно основание се предвижда съвместно обработване на данните за обща цел.

Пример: База данни, съвместно управлявана от няколко кредитни институции при работата им с техни неизправни клиенти, е често срещан пример за съвместно обработване на лични данни от повече от един администратор. Когато някой кандидатства за кредитиране от банка, която е един от съвместните администратори, банките проверяват базата данни, за да получат информация при вземането на информирани решения за кредитоспособността на кандидата.

В разпоредбите не е изрично записано дали съвместното обработване на лични данни от повече от един администратор изисква целта да бъде една и съща за всеки един от администраторите или е достатъчно техните цели да се припокриват само частично. Въпреки това, все още не съществува приложима съдебна практика на европейско равнище и липсва яснота относно последствията във връзка с отговорността. Работната група по член 29 се застъпва за по-широко тълкуване на понятието за съвместно обработване на

84 Вж. също Работна група за защита на личните данни по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни" и „лице, което обработва данните"*, WP 169, Брюксел, 16 февруари 2010 г., стр. 15.

85 Директива за защита на личните данни, член 2, буква г).

лични данни от повече от един администратор с цел да се даде възможност за известна гъвкавост, за да бъде предвидена увеличаващата се сложност на настоящото действително положение с обработването на данни[86]. Дело, свързано със Дружеството за световна междубанкова финансова телекомуникация (SWIFT), илюстрира позицията на Работната група.

Пример: В така наречената дело SWIFT европейските банкови институции са използвали SWIFT, първоначално като обработващи, за да осъществяват трансферът на данни в хода на банковите транзакции. SWIFT е разкрило на Министерството на финансите на САЩ данни за банкови транзакции, съхранявани в изчислителен център в Съединените щати, без това да му е било изрично разпоредено от европейските банкови институции, които са използвали услугите му. При оценяване на законосъобразността на тази ситуация Работната група по член 29 е стигнала до заключението, че европейските банкови институции, използващи SWIFT, както и самото дружество SWIFT, е трябвало да се разглеждат като съвместни администратори, отговорни пред европейските клиенти за разкриването на техни данни на органите на САЩ[87]. Като е решило да разкрие данните, SWIFT е поело — незаконно — ролята на администратор; банковите институции очевидно не са изпълнили задължението си да упражняват надзор върху своя обработващ и поради това не могат да бъдат напълно освободени от носената от тях отговорност в качеството им на администратори. Това положение води до съвместно обработване на лични данни от повече от един администратор.

Обработващ

Съгласно правото на ЕС „обработващ" означава лице, което обработва лични данни от името на администратора[88]. Дейностите, възложени на един обработващ, могат да бъдат ограничени до много специфична задача или цел, или могат да са доста общи и всеобхватни.

86 Работна група за защита на личните данни по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни" и „лице, което обработва данните"*, WP 169, Брюксел, 16 февруари 2010 г., стр. 19.

87 Работна група за защита на личните данни по член 29 (2006 г.), *Становище 10/2006 относно обработката на лични данни от Дружеството за световна междубанкова финансова телекомуникация (SWIFT)*, WP 128, Брюксел, 22 ноември 2006 г.

88 Директива за защита на личните данни, член 2, буква д).

Съгласно правото на Съвета на Европа значението на понятието „обработващ" е същото като в правото на ЕС.

Обработващите данни лица, освен че обработват данни за други лица, също ще бъдат администратори по отношение на обработването, което извършват за свои собствени цели, например администрирането на своите собствени служители, продажби и сметки.

Примери: Дружеството Everready е специализирано в областта на обработването на данни за управление на човешките ресурси на други дружества. В тази си функция Everready е обработващ.

Когато Everready обработва данните на собствените си служители, то обаче е администратор на операциите по обработването на данни за целите на изпълнението на своите задължения като работодател.

Връзката между администратор и обработващ

Както е видно, администраторът е този, който определя целите и средствата на обработването.

Пример: Директорът на дружеството Sunshine решава, че дружество Moonlight, специалист по маркетингово проучване, следва да извърши пазарно проучване на данни на клиентите на Sunshine. Въпреки че, по този начин, задачата за определяне на средствата за обработване ще бъде делегирана на Moonlight, дружеството Sunshine продължава да бъде администраторът на данните, а Moonlight е само обработващ, тъй като според договора Moonlight може да използва данните на клиентите на дружеството Sunshine само за определени от Sunshine цели.

Дори ако правомощието за определяне на средствата за обработване е делегирано на обработващ, администраторът трябва да може да се намесва в решенията на обработващия по отношение на средствата за обработване. Цялостната отговорност се носи от администратора, който трябва да упражнява надзор над обработващите, за да гарантира, че техните решения съответстват на законодателството за защита на данните. Договор, в който се забранява на администратора да се намесва в решенията на обработващия, вероятно ще се тълкува като имащ за резултат съвместно обработване на

лични данни от повече от един администратор, при което двете страни си поделят правната отговорност на администратор.

Освен това, ако обработващият не зачита определените от администратора ограничения по отношение на използването на данните, то обработващият се превръща в администратор поне в степента, в която е нарушил указанията на администратора. Това най-вероятно ще превърне обработващия в администратор, който действа незаконосъобразно. От своя страна, първоначалният администратор ще трябва да обясни как е било възможно обработващият да наруши неговите нареждания. Действително, има тенденция Работната група по член 29 в такива случаи да приема, че е налице съвместно обработване на лични данни от повече от един администратор, тъй като това осигурява най-добра защита на интересите на физическите лица[89]. Важна последица от съвместното обработване на лични данни от повече от един администратор следва да бъде солидарната отговорност за вреди, като по този начин на физическите лица се предоставя по-широк кръг от средства за правна защита.

Също така, може да съществуват проблеми във връзка с разпределянето на отговорността в случаите, в които администраторът е малко предприятие, а обработващият е голяма корпорация, която има правомощието да диктува условията за своите услуги. При такива обстоятелства обаче, Работната група по член 29 твърди, че стандартът по отношение на отговорността не следва да се занижава въз основа на липсата на икономическо равновесие и че трябва да се запази разбирането за понятието „администратор“[90].

За по-голяма яснота и прозрачност подробностите за отношенията между администратора и обработващия трябва да бъдат документирани в писмен договор[91]. Липсата на подобен договор е нарушение на задължението на

89 Работна група за защита на личните данни по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни“ и „лице, което обработва данните“*, WP 169, Брюксел, 16 февруари 2010 г., стр. 25; и Работна група за защита на личните данни по член 29 (2006 г.), *Становище 10/2006 относно обработката на лични данни от Дружеството за световна междубанкова финансова телекомуникация (SWIFT)*, WP 128, Брюксел, 22 ноември 2006 г.

90 Работна група за защита на личните данни по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни“ и „лице, което обработва данните“*, WP 169, Брюксел, 16 февруари 2010 г., стр. 26.

91 Директива за защита на личните данни, член 17, параграфи 3 и 4.

администратора да предоставя писмена документация относно общите отговорности и може да доведе до налагане на санкции[92].

Обработващите може да проявят желание да делегират определени задачи на допълнителни обработващи, действащи като подизпълнители. По закон това е допустимо и ще зависи в детайли от договорните клаузи между администратора и обработващия, включително и от това дали е необходимо разрешението на администратора за всеки отделен случай или дали информирането само по себе си е достатъчно.

Съгласно правото на Съвета на Европа- обясненото по-горе,тълкуване на понятията „администратор" и „обработващ" е напълно приложимо, както е видно от препоръките, изготвени съгласно Конвенция № 108[93].

2.3.2. Получатели и трети лица

Разликата между тези две категории лица или субекти, които бяха въведени с Директивата за защита на личните данни, се състои най-вече във връзката им с администратора, а оттам и в разрешението им за достъп до съхраняваните от администратора лични данни.

„Трето лице" е лице, което е с различна правосубектност от администратора. Поради това, винаги ще е необходимо специално правно основание за разкриването на данни на трето лице. Съгласно член 2, буква е) от Директивата за защита на личните данни „трето лице" означава „всяко физическо или юридическо лице, държавен орган, агенция или друг орган, различни от съответното физическо лице, администратора, обработващия данните и лицата, които под прякото ръководство на администратора или обработващия данните, имат право да обработват данните". Това означава, че лица, работещи за организация, която е с различна правосубектност от администратора, дори ако тя принадлежи към същата група или холдинг, са (или принадлежат към) „трети лица". От друга страна, „клоновете на банка, която обработва

92 Работна група за защита на личните данни по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни" и „лице, което обработва данните"*, WP 169, Брюксел, 16 февруари 2010 г., стр. 27.

93 Вж. например Препоръката относно профилирането, член 1.

сметки на клиент под прякото ръководство на своето главно управление, не са трети лица“[94].

Терминът „получател“ е по-широк от термина „трето лице“. По смисъла на член 2, буква ж) от Директивата за защита на личните данни „получател“ означава „физическо или юридическо лице, държавен орган, агенция или друг орган, пред които се разкриват данни, независимо дали е трето лице или не“. Този получател може да бъде или лице извън организацията на администратора или обработващия — тогава той би бил трето лице, — или някой вътре в организацията на администратора или обработващия, като например служител или друг отдел в рамките на същото дружество или орган.

Разграничението между получатели и трети лица е важно само заради условията за законосъобразно разкриване на данни. Служителите на даден администратор или обработващ могат, без наличието на допълнително правно изискване, да бъдат получатели на лични данни, ако те участват в операциите по обработване, извършвани от администратора или обработващия. От друга страна, на третото лице, тъй като е отделен от администратора или обработващия данни, юридически субект, не е разрешено да използва личните данни, обработвани от администратора, освен при наличието на специални правни основания в конкретния случай. Поради това „получателите на данните — трети лица“ винаги ще се нуждаят от правно основание, за да получат законно лични данни.

Пример: Служител на обработващия, който използва лични данни в рамките на изпълнение на задачите, възложени му от работодателя, е получател на данните, но не е трето лице, тъй като той използва данните от името на и съгласно указанията на обработващия.

Ако обаче същият служител реши да използва данните, до които може да има достъп в качеството си на служител на обработващия, за свои собствени цели и ги продаде на друго дружество, тогава служителят действа като трето лице. Той вече не следва нарежданията на обработващия (работодателя). Като трето лице служителят ще се нуждае от правно основание за придобиването и продажбата на данните. В този пример служителят със сигурност няма такова правно основание, така че тези действия са незаконни.

94 Работна група за защита на личните данни по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни“ и „лице, което обработва данните“*, WP 169, Брюксел, 16 февруари 2010 г., стр. 31.

2.4. Съгласие

Ключови въпроси

- Съгласието като правно основание за обработването на лични данни трябва да бъде свободно изразено, конкретно и информирано.
- Съгласието трябва да е било дадено недвусмислено. Съгласието може да бъде дадено или изрично, или мълчаливо — като се действа по начин, който не оставя никакво съмнение, че физическото лице е съгласно с обработването на неговите данни.
- За обработването на чувствителни данни въз основа на дадено съгласие е необходимо предоставянето на изрично съгласие.
- Съгласието може да бъде оттеглено по всяко време.

„Съгласие“ означава „всяко свободно изразено, конкретно и информирано указание за волята на съответното физическо лице“[95]. В редица случаи то е правното основание за законосъобразното обработване на данните (вж. раздел раздел 4.1).

2.4.1. Елементите на валидното съгласие

Правото на ЕС предвижда три елемента, при наличието на които дадено съгласие е валидно, с които се цели да се гарантира, че физическите лица действително са имали намерение да дадат съгласието си за използването на техните данни:

- физическото лице не трябва да бъде под какъвто и да било натиск, когато изразява съгласието си;
- физическото лице трябва да е било надлежно информирано относно правото на възражение и последиците от изразяване на съгласие; и
- обхватът на съгласието трябва да бъде достатъчно конкретен.

По смисъла на правото зазащита на данните съгласието ще бъде валидно само ако всички тези изисквания бъдат изпълнени.

95 Директива за защита на личните данни, член 2, буква з).

В Конвенция № 108 не се съдържа определение за съгласие; такова е дадено в националното законодателство. Въприки това,**съгласно правото на Съвета на Европа,** елементите на валидното съгласие съответстват на пояснените по-горе, , както е предвидено в препоръките, изготвени съгласно Конвенция № 108[96]. Изискванията за съгласие са същите като изискванията за валидна декларация за намерение, заложени в европейското гражданско право.

Допълнителните изисквания за валидно съгласие съгласно гражданското право, каквото е изискването за правоспособност, естествено също се прилагат в контекста на защита на данните, тъй като те са основни правни предпоставки. Невалидното съгласие на лица, които нямат правоспособност, ще доведе до липса на правно основание за обработване на данни за тези лица.

Съгласието може да бъде дадено или изрично[97], или мълчаливо. Изричното съгласие не поражда каквито и да било съмнения относно намеренията на физическите лица и то може да бъде дадено или в устна, или в писмена форма; за даването на мълчаливо съгласие извод се прави съобразно обстоятелствата. Всяко съгласие трябва да бъде дадено недвусмислено[98]. Това означава, че не следва да има каквото и да било основателно съмнение за това дали физическото лице имало желание да съобщи своето съгласие за обработване на неговите данни. Например, извод за недвусмислено съгласие не може да се направи просто въз основа на бездействие. Когато данните, подлежащи на обработване, са чувствителни, изричното съгласие е задължително и то трябва да бъде недвусмислено.

Свободно изразено съгласие

Наличието на свободно изразено съгласие е валидно само „ако субектът на данни е в състояние да направи действителен избор и не съществува риск от измама, заплашване, принуда или съществени отрицателни последствия, ако той/тя не изрази съгласие“[99].

96 Вж. например Конвенция № 108, Препоръка относно статистическите данни, точка 6.

97 Директива за защита на личните данни, член 8, параграф 2.

98 *Пак там*,член 7, буква а) и член 26, параграф 1.

99 Вж. също Работна група за защита на личните данни по член 29 (2011 г.), *Становище 15/2011 относно понятието „съгласие“*, WP 187, Брюксел, 13 юли 2011 г., стр. 12.

Пример: На много летища е необходимо пътниците да преминават през скенери за проверка на хора, за да бъдат допуснати до зоната за качване на борда на самолета[100]. Като се има предвид, че данните на пътниците се обработват по време на сканирането, обработването трябва да отговаря на едно от правните основания съгласно член 7 от Директивата за защита на личните данни (вж. раздел 4.1.1). Преминаването през скенери за проверка на хора понякога се представя на пътниците като незадължително изискване, което предполага, че тяхното съгласие може да обоснове обработването. При все това е възможно пътниците да се страхуват, че отказът им да преминат през скенери за проверка на хора ще породи съмнение или че ще доведе до допълнителни проверки като личен обиск. Много хора дават съгласието си за преминаване през скенер, за да избегнат възможни проблеми или закъснения. Както става ясно, такова съгласие не е изразено свободно в достатъчна степен.

От това следва, че солидно законно основание може да бъде намерено само в законодателен акт въз основа на член 7, буква д) от Директивата за защита на личните данни, който поражда задължение за пътниците да сътрудничат в името на по-висш обществен интерес. Това законодателство все пак може да предвижда избор между сканиране и личен обиск, но само като част от допълнителни мерки за граничен контрол, които са необходими при конкретни обстоятелства. Именно това беше определено от Европейската комисия през 2011 г. в два регламента, които обхващат скенерите за целите на сигурността[101].

Свободно изразеното съгласие би могло да бъде застрашено също така в положение на подчиненост, когато е налице значителна икономическа или друг вид неравнопоставеност между администратора, който осигурява съгласието, и физическото лице, което дава съгласието[102].

100 Този пример е взет от *пак там*, стр. 15

101 Регламент (ЕС) № 1141/2011 на Комисията от 10 ноември 2011 г. за изменение на Регламент (ЕО) № 272/2009 за допълване на общите основни стандарти за сигурност на гражданското въздухоплаване, отнасящо се за използването в летищата на ЕС на скенери за целите на сигурността, ОВ L 293, 11.11.2011 г., и Регламент (ЕС) № 1147/2011 за изпълнение на Комисията от 11 ноември 2011 г. за изменение на Регламент (ЕС) № 185/2010 за прилагане на общите основни стандарти за сигурност във гражданското въздухоплаване, във връзка с използването в летищата на ЕС на скенери за целите на сигурността, ОВ L 294, 12.11.2011 г.

102 Вж. също Работна група за защита на личните данни по член 29 (2001 г.), *Opinion 8/2001 on the processing of personal data in the employment context [Становище 8/2001 относно обработването на личните данни в контекста на трудовите правоотношения]*, WP 48, Брюксел, 13 септември 2001 г.; и Работна група за защита на личните данни по член 29 (2005 г.), Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995 [Работен документ за общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г.], WP 114, Брюксел, 25 ноември 2005 г.

Пример: Голямо дружество планира да създаде указател, съдържащ имената на всички служители, длъжността, която те заемат в дружеството, и служебните им адреси единствено с цел подобряване на комуникацията в рамките на дружеството. Ръководителят на отдел „Човешки ресурси“ предлага в указателя да бъде добавена снимка на всеки служител с цел да се улесни разпознаването на колеги на срещи. Представители на служителите искат това да бъде направено само ако отделният служител даде съгласието си за подобно нещо.

В тази ситуация съгласието на служител следва да бъде счетено за правно основание за обработване на снимките в указателя, тъй като е ясно, че няма отрицателни последици от това дадена снимка да бъде публикувана в указател и освен това е възможно служителят да не бъде засегнат от предизвиканите от работодателя отрицателни последици, ако не даде съгласието си негова снимка да бъде публикувана в указателя.

Това обаче не означава, че съгласието никога не може да бъде валидно при обстоятелства, при които отказът да се даде съгласие би имал отрицателни последици. Ако например не бъде дадено съгласие за издаване на клиентска карта за супермаркет, това води само до неполучаване на отстъпки от цените на определени стоки, съгласието все пак представлява валидно правно основание за обработване на личните данни на онези клиенти, които са дали съгласието си за издаване на такава карта. Не е налице положение на подчиненост между дружество и клиент, а последиците от отказа да се даде съгласие не са достатъчно сериозни за физическото лице, така че да попречат на свободния избор.

От друга страна, всеки път, когато важни стоки или услуги могат да бъдат получени само и единствено ако определени лични данни бъдат разкрити на трети лица, съгласието на физическото лице за разкриването на неговите данни обикновено не може да бъде считано за свободно изразено и следователно не е валидно съгласно правото за защита на данните.

Пример: Съгласие, изразено от пътниците пред авиокомпания, за трансфера от нея на така наречените резервационни данни на пътниците (PNR), а именно данни относно тяхната самоличност, хранителни навици или здравословни проблеми, към имиграционните органи на конкретна чужда държава не може да бъде счетено за валидно съгласие съгласно

правото за защита на данните, тъй като пътуващите лица нямат никакъв избор, ако желаят да посетят тази държава. За да бъде трансферът на тези данни законосъобразен, се изисква друго правно основание, различно от съгласие: най-вероятно специален закон.

Информирано съгласие

Физическото лице трябва да разполага с достатъчно информация преди да вземе своето решение. Дали предоставената информация е достатъчна може да бъде преценено за всеки конкретен случай. Обикновено информираното съгласие включва точно и лесно разбираемо описание на въпроса, по отношение на който се изисква съгласие, и в допълнение, очертава последиците от даването или отказът да се даде съгласие. Езикът, който трябва да се използва при предоставянето на информация, следва да бъде съобразен с предвидените адресати на информацията.

Освен това, информацията трябва да бъде лесно достъпна за физическото лице. Достъпността и видимостта на информацията са важни елементи. В онлайн среда „многостепенните" съобщения могат да бъдат добро решение, тъй като, в допълнение към кратко представяне на информацията, физическото лице може да има достъп и до едно по-подробно представяне на информацията.

Конкретно съгласие

За да бъде валидно, съгласието трябва да бъде и конкретно. Това върви ръка за ръка с качеството на информацията, предоставена относно обекта на съгласие. В тази връзка са важни основателните очаквания на едно средностатистическо физическо лице. От физическото лице, още веднъж, може да бъде поискано да даде съгласието си, ако предстои добавяне на операции по обработване или промяната им по начин, който не е могъл да бъде добре предвиденпри даване на първоначалното съгласие.

Пример: В делото *Deutsche Telekom AG*[103] Съдът на ЕС е разгледал въпроса дали доставчикът на телекомуникационни услуги, който е трябвало да предоставя лични данни на абонатите съгласно член 12 от *Директивата*

103 Съд на ЕС, Решение от 5 май 2011 г. по дело *Deutsche Telekom AG/Bundesrepublik Deutschland*, C-543/09; вж. по-специално точки 53 и 54.

за правото на неприкосновеност на личния живот и електронни комуникации[104], е имал нужда от подновено съгласие от физическите лица, тъй като при първоначалното даване на съгласие не са били посочени имената на получателите на услугата.

Съдът на ЕС е постановил, че съгласно този член, не е било необходимо подновено съгласие преди предаване на данните, тъй като съгласно тази разпоредба, физическите лица са имали възможността да се съгласят само с целта на обработването, която е публикуване на техните данни, и не са могли да избират между различните директории, в които тези данни могат да бъдат публикувани.

Както Съдът подчерта „при тълкуването на член 12 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации с оглед на контекста и систематичното място на тази разпоредба се налага изводът, че съгласието по смисъла на параграф 2 от този член се отнася до целта на публикуването на личните данни в публичния указател, а не до издаването им от конкретен доставчик на указатели“[105]. Освен това „вреди за абоната би могло да причини именно публикуването на личните данни в указател, който има особена цел“[106], а не това кой е авторът на това публикуване.

2.4.2. Правото на оттегляне на съгласие по всяко време

В Директивата за защита на личните данни не се посочва общо право за оттегляне на съгласие по всяко време. Въпреки това е широко разпространено предположението, че такова право съществува и физическото лице трябва да може да го упражнява по своя преценка. Не следва да съществува каквото и да било изискване за посочване на причини за оттеглянето, както и какъвто и да било риск от отрицателни последици, превишаващи възможните ползи, произтичащи от даденото по-рано съгласие за използване на данните.

104 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации, ОВ L 201, 31.7.2002 г. (*Директива за правото на неприкосновеност на личния живот и електронни комуникации*).

105 Съд на ЕС, Решение от 5 май 2011 г. по дело *Deutsche Telekom AG/Bundesrepublik Deutschland*, C-543/09; вж. по-специално точка 61.

106 *Пак там*, вж. по-специално точка 62.

Пример: Клиент дава съгласие за получаване на рекламно-информационни съобщения, изпращани на адрес, предоставен от този клиент на администратора на данни. Ако клиентът оттегли своето съгласие, администраторът трябва незабавно да спре да изпраща рекламно-информационни съобщения. Оттеглянето няма да има за своя последица каквито и да било наказания като плащане на такси.

Ако даден клиент е използвал отстъпка от 5 % от цената за ползване на хотелска стая срещу даването на съгласие от негова страна за използване на данните му за изпращане на рекламно-информационни съобщения, оттеглянето на съгласие за получаване на такива съобщения на по-късен етап не следва да породи задължение за възстановяване на тези отстъпки от клиента.

3

Основните принципи на европейското право в областта на защитата на данните

ЕС	Обхванати въпроси	Съвет на Европа
Директива за защита на личните данни, член 6, параграф 1, букви а) и б) Съд на ЕС, Решение от 16 декември 2008 г. по дело *Huber/Германия*, C-524/06 Съд на ЕС, Решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR (C-92/09) u Hartmut Eifert (C-93/09)/Land Hessen*, съединени дела C-92/09 и C-93/09	**Принципът за законосъобразно обработване**	Конвенция № 108, член 5, букви а) и б) ЕСПЧ, Решение от 4 май 2000 г. по дело *Rotaru/Румъния* [голям състав], № 28341/95 ЕСПЧ, Решение от 22 октомври 2002 г. по дело *Taylor-Sabori/Обединеното кралство*, № 47114/99 ЕСПЧ, Решение от 28 януари 2003 г. по дело *Peck/Обединеното кралство*, № 44647/98 ЕСПЧ, Решение от 18 октомври 2011 г. по дело *Khelili/Швейцария*, № 16188/07 ЕСПЧ, Решение от 26 март 1987г. по дело *Leander/Швеция*, № 9248/81
Директива за защита на личните данни, член 6, параграф 1, буква б)	**Принципът за определяне и ограничаване на целта**	Конвенция № 108, член 5, буква б)

	Принципите за качество на данните:	
Директива за защита на личните данни, член 6, параграф 1, буква в)	Съотносимост на данните	Конвенция № 108, член 5, буква в)
Директива за защита на личните данни, член 6, параграф 1, буква г)	Точност на данните	Конвенция № 108, член 5, буква г)
Директива за защита на личните данни, член 6, параграф 1, буква д)	Лимитиран период на запазване на данни	Конвенция № 108, член 5, буква д)
Директива за защита на личните данни, член 6, параграф 1, буква д)	Изключение за научноизследователски и статистически цели	Конвенция № 108, член 9, параграф 3
Директива за защита на личните данни, член 6, параграф 1, буква а)	Принципът за добросъвестно обработване	Конвенция № 108, член 5, буква а) ЕСПЧ, Решение от 27 октомври 2009 г. по дело *Haralambie / Румъния*, № 21737/03 ЕСПЧ, Решение от 6 ноември 2009 г. по дело *K.H и други/Словакия*, № 32881/04
Директива за защита на личните данни, член 6, параграф 2	Принципът за отчетност	

Принципите, изложени в член 5 от Конвенция № 108, утвърждават основния характерна европейското право в областта на защитата на данните. Те присъстват и в член 6 от Директивата за защита на личните данни като отправна точка за по-подробни разпоредби в последващите членове от директивата. Цялото последващо законодателство в областта на защитата на данните на Съвета на Европа или на ЕС трябва да отговаря на тези принципи и те трябва да се вземат предвид при тълкуването на това законодателство. Всякакви изключения от и ограничения на тези основни принципи могат да бъдат предвидени на национално равнище[107]; те трябва да бъдат предвидени от закона, с тях да се преследва законна цел и те да бъдат необходими в едно демократично общество. Трябва да бъдат изпълнени всичките три условия.

107 Конвенция № 108, член 9, параграф 2; Директива за защита на личните данни, член 13 във връзка с член 9, параграф 2.

3.1. Принципът за законосъобразно обработване

Ключови въпроси

- За да се разбере принципът за законосъобразно обработване, трябва да се направи позоваване на условията за законните ограничения на правото на защита на данните в контекста на член 52, параграф 1 от Хартата и изискванията за обоснована намеса съгласно член 8, параграф 2 от ЕКПЧ.
- Съответно обработването на лични данни е законосъобразно само ако то:
  - е в съответствие със закона; и
  - с него се преследва законна цел; и
  - е необходимо в едно демократично общество, за да се постигне законната цел.

Съгласно правото на ЕС и на Съвета на Европа в областта на защитата на данните принципът за законосъобразно обработване е първият посочен принцип; той е представен с почти еднаква формулировка в член 5 от Конвенция № 108 и в член 6 от Директивата за защита на личните данни.

Нито една от тези разпоредби не съдържа определение на това какво представлява „законосъобразното обработване". За да се разбере този правен термин, е необходимо да се направи позоваване на обоснованата намеса съгласно ЕКПЧ, както е дадено тълкуване за нея в съдебната практика на ЕСПЧ, и на условията за законните ограничения съгласно член 52 от Хартата.

3.1.1. Изискванията за обоснована намеса съгласно ЕКПЧ

Обработването на лични данни може да представлява намеса в правото на неприкосновеност на личния живот на физическото лице. Правото на неприкосновеностна личния живот обаче не е абсолютно право, а трябва да бъде балансирано и съвместявано с други законни интереси, независимо дали те са на други лица (частни интереси) или на обществото като цяло (обществени интереси). Условията, при които държавната намеса е обоснована, са следните:

Намесата е в съответствие със закона

Съгласно съдебната практика на ЕСПЧ, намесата е в съответствие със закона, ако се основава на разпоредба от националното законодателство, която има определени характеристики. Законовата разпоредба трябва „да бъде достъпна за съответното лице и предвидима по отношение на своите последици“[108]. Една разпоредба е предвидима, „ако е формулирана с достатъчна точност, за да позволи на всяко лице — ако е необходимо с подходяща консултация — да съобрази с нея поведението си“[109]. „Степента на точност, изисквана от „закона“в тази връзка ще зависи от конкретния въпрос“[110].

Пример: В дело *Rotaru/Румъния*[111] ЕСПЧ е установил нарушение на член 8 от ЕКПЧ, тъй като законодателството на Румъния допуска събирането, записването и архивирането на секретни досиета с информация, засягаща националната сигурност, без да бъдат поставяни ограничения за упражняването на тези правомощия, което се извършва по усмотрението на органите. Например в националното законодателство не са били определени типът информация, която може да бъде обработвана, категориите хора, срещу които могат да бъдат взети мерки за наблюдение, обстоятелствата, при които могат да бъдат взети тези мерки, или процедурата, която трябва да бъде следвана. Поради тези недостатъци, Съдът е заключил, че националното законодателство не отговаря на изискванията за предвидимост по член 8 от ЕКПЧ и че този член е нарушен.

108 ЕСПЧ, Решение от 16 февруари 2000 г. по дело *Amann/Швейцария* [голям състав], № 27798/95, точка 50; вж. също ЕСПЧ, Решение от 25 март 1998 г. по дело *Kopp/Швейцария*, № 23224/94, точка 55 и ЕСПЧ, Решение от 10 февруари 2009 г. по дело *Iordachi и други/Молдова*, № 25198/02, точка 50.

109 ЕСПЧ, Решение от 16 февруари 2000 г. по дело *Amann/Швейцария* [голям състав], № 27798/95, точка 56; вж. също ЕСПЧ, Решение от 26 април 1985 г. по дело *Malone/Обединеното кралство*, № 8691/79, точка 66; ЕСПЧ, Решение от 25 март 1983 г. по дело *Silver и други/Обединеното кралство*, № 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, точка 88.

110 ЕСПЧ, Решение от 26 април 1979 г. по дело *The Sunday Times/Обединеното кралство*, № 6538/74, точка 49; вж. също ЕСПЧ, Решение от 25 март 1983 г. по дело *Silver и други/Обединеното кралство*, № 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, точка 88.

111 ЕСПЧ, Решение от 4 април 2000 г. по дело *Rotaru/Румъния* [голям състав], № 28341/95, точка 57; вж. също ЕСПЧ, Решение от 28 юни 2007 г. по дело *Асоциация за Европейска интеграция и права на човека и Екимджиев/България*, № 62540/00; ЕСПЧ, Решение от 21 юни 2011 г. по дело *Shimovolos/Русия*, № 30194/09; и ЕСПЧ, Решение от 31 май 2005 г. по дело *Vetter/Франция*, № 59842/00.

Пример: В дело *Taylor-Sabori/Великобритания*[112] жалбоподателят е бил обект на полицейско наблюдение. Посредством използване на „клонинг" на пейджъра на жалбоподателя полицията е била в състояние да прихваща съобщенията, изпратени до него. След това жалбоподателят е бил арестуван и обвинен в конспирация за доставяне на контролирани наркотици. Част от наказателното преследване срещу него се е състояло в писмени записи на съобщенията от пейджъра от този период, които са били възпроизведени в писмена форма от полицията. Въпреки това по време на съдебния процес на жалбоподателя в британския закон не е съществувала клауза, която да урежда прихващането на съобщения, предадени чрез частна телекомуникационна система. Поради това нарушаването на неговите права не е било „в съответствие със закона". ЕСПЧ е заключил, че е налице нарушение на член 8 от ЕКПЧ.

Преследване на законна цел

Законната цел може да бъде свързана с посочените обществени интереси или с правата и свободите на други лица.

Пример: В делото *Peck/Великобритания*[113] жалбоподателят е направил опит за самоубийство на улицата, като е прерязал вените на ръцете си, без да знае, че камерата на система за видеонаблюдение (CCTV) го е заснела по време на опита. След като полицията, която е наблюдавала камерите на CCTV, го е спасила, полицейските органи са предали кадрите от CCTV на медиите, които са ги публикували без да скрият лицето на жалбоподателя. ЕСПЧ е заключил, че не са налице уместни или достатъчни причини, които да оправдаят факта, че органите директно са разкрили кадрите на обществеността, без да са получили съгласието на жалбоподателя или без да скрият неговата самоличност. Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

112 ЕСПЧ, Решение от 22 октомври 2002 г. по дело *Taylor-Sabori/Обединеното кралство*, № 47114/99.

113 ЕСПЧ, Решение от 28 януари 2003 г. по дело *Peck/Обединеното кралство*, № 44647/98, по-специално точка 85.

Намесата е необходима в едно демократично общество

ЕСПЧ е постановил, че „концепцията за необходимост предполага, че намесата съответства на належаща обществена нужда, и по-специално, че тя е пропорционална на преследваната законна цел“[114].

Пример: В делото *Khelili/Швейцария*[115] по време на полицейска проверка полицията е установила, че жалбоподателката носи визитни картички, на които пише: „Красива жена над 35 би искала да се срещне с мъж за по питие или с цел срещи от време на време. Тел. номер. [...]“. Жалбоподателката твърдяла, че след това разкритие полицията е регистрирала името ѝ в архивите си като проститутка — дейност, която тя постоянно отричала. Жалбоподателката поискала думата „проститутка“ да бъде изтрита от компютърните регистри. ЕСФЧ принципно е признал, че задържането на личните данни на дадено лице на основание, че то би могло да извърши друго правонарушение, би могло при определени обстоятелства да е пропорционално. Но в случая на жалбоподателката твърдението за незаконна проституция изглежда твърде неясно и общо, като не е подкрепено от конкретни факти, тъй като тя никога не е била обвинена в незаконна проституция и следователно не може да бъде считано, че удовлетворява „належаща обществена нужда“ по смисъла на член 8 от ЕПКЧ. Приемайки това като въпрос, по отношение на който органите трябва да докажат точността на съхранените данни за жалбоподателката, и предвид сериозността на намесата в правата на жалбоподателката, Съдът е постановил, че запазването на думата „проститутка“ в полицейските досиета в продължение на години не е било необходимо в едно демократично общество. Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

Пример: По делото *Leander/Швеция*[116] ЕСЧП е постановил, че тайното проучване на лица, които кандидатстват за назначаване на важни постове в областта на националната сигурност само по себе си не е в противоречие с изискването за необходимост в едно демократично общество. Специалните гаранции, предвидени в националното законодателство за защита на интереса на съответното физическо лице, например, контролът,

114 ЕСПЧ, Решение от 11 юли 1985 г. по дело *Leander/Швеция*, № 9248/81, точка 58.

115 ЕСПЧ, Решение от 18 октомври 2011 г. по дело *Khelili/Швейцария*, № 16188/07.

116 ЕСПЧ, Решение от 11 юли 1985 г. по дело *Leander/Швеция*, № 9248/81, точки 59 и 67.

упражняван от Парламента и министъра на правосъдието, са довели до заключението на ЕСПЧ, че шведската система за контрол на персонала отговаря на изискванията на член 8, параграф 2 от ЕКПЧ. Като е взела предвид голямата свобода на преценка, с която разполага, държавата ответник е имала правото да счете, че в случая на жалбоподателя интересите на националната сигурност имат преимущество над личните интереси. Съдът е заключил, че не е налице нарушение на член 8 от ЕКПЧ.

3.1.2. Условията за законни ограничения съгласно Хартата на ЕС

Структурата и формулировката на Хартата е различна от тази на ЕКПЧ. В Хартата не се говори за намеса в гарантираните права, а се съдържа разпоредба относно ограничението(ята) на упражняването на правата и свободите, признати от Хартата.

Съгласно член 52, параграф 1 ограниченията на упражняването на правата и свободите, признати от Хартата, и съответно, и на упражняването на правото на защита на личните данни, като например обработването на лични данни, са допустими само ако тези ограничения:

- са предвидени в закон; и
- зачитат основния характер на правото на защита на данните; и
- са необходими, при спазване на принципа на пропорционалност; и
- отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

Примери: В решението по дело *Volker u Markus Schecke*[117] Съдът на ЕС заключи, че с наложеното от тях задължение за публикуване на лични данни относно всяко физическо лице, което е било бенефициент на помощи [от определени земеделски фондове], без да правят разграничение въз основа на релевантни критерии като периодите, през които те са получавали подобни помощи, честотата или вида и размера на

117 Съд на ЕС, Решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR (C-92/09) u Hartmut Eifert (C-93/09)/Land Hessen*, съединени дела C-92/09 и C-93/09, точки 89 и 86.

помощите, Съветът и Комисията са надхвърлили границите, наложени от спазването на принципа на пропорционалност.

Поради това, Съдът на ЕС прие за необходимо да обяви за недействителни някои разпоредби на Регламент (ЕО) № 1290/2005 на Съвета и да декларира Регламент (ЕО) № 259/2008 за недействителен в неговата цялост[118].

Въпреки различната формулировка условията за законосъобразно обработване, посочени в член 52, параграф 1 от Хартата, напомнят на член 8, параграф 2 от ЕКПЧ. Действително условията, изброени в член 52, параграф 1 от Хартата, трябва да се разглеждат като съответстващи на тези, посочени в член 8, параграф 2 от ЕКПЧ, тъй като в първото изречение на член 52, параграф 3 от Хартата се посочва, че „доколкото настоящата Харта съдържа права, съответстващи на права, гарантирани от Европейската конвенция за защита на правата на човека и основните свободи, техният смисъл и обхват са същите като дадените им в посочената Конвенция".

Съгласно последното изречение от член 52, параграф 3 обаче „тази разпоредба не пречи правото на Съюза да предоставя по-широка защита". В контекста на сравняване на член 8, параграф 2 от ЕКПЧ и първото изречение на член 52, параграф 3 това може само да означава, че условията за обоснована намеса съгласно член 8, параграф 2 от ЕКПЧ са минималните изисквания за законните ограничения на правото на защита на данните съгласно Хартата. Следователно, съгласно правото на ЕС, законосъобразното обработване на лични данни изисква да бъдат изпълнени поне условията, посочени в член 8, параграф 2 от ЕКПЧ; правото на ЕС, обаче, може да определя допълнителни изисквания за специални случаи.

Съответствието на принципа за законосъобразно обработване, заложен вправото на ЕС, със съответните разпоредби на ЕКПЧ се насърчава допълнително в член 6, параграф 3 от Договора за ЕС, при условие че „основните права, както са гарантирани от Европейската конвенция за защита на правата на човека и основните свободи [...], са част от правото на Съюза в качеството им на общи принципи".

118 Регламент (ЕО) № 1290/2005 на Съвета от 21 юни 2005 г. относно финансирането на Общата селскостопанска политика, ОВ L 209, 11.8.2005 г.; Регламент (ЕО) № 259/2008 на Комисията от 18 март 2008 г. за установяване на подробни правила за прилагане на Регламент (ЕО) № 1290/2005 относно публикуването на информация за получателите на средства от Европейския фонд за гарантиране на земеделието (ЕФГЗ) и Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР), ОВ L 76, 19.3.2008 г.

3.2. Принципът за определяне и ограничаване на целта

Ключови въпроси

- Целта на обработването на данните трябва да бъде ясно определена преди започване на обработването.
- Съгласно правото на ЕС целта на обработването трябва да бъдеизрично определена; съгласно правото на Съвета на Европа този въпрос е оставен на националното законодателство.
- Обработването за неопределени цели не е в съответствие с правото за защита на данните.
- За по-нататъшно използване на данните за друга цел се изисква допълнително правно основание, ако новата цел на обработването е несъвместима с първоначалната цел.
- Трансферът на данни към трети лица е нова цел, за която се изисква допълнително правно основание.

По същество принципът за определяне и ограничаване на целта означава, че законосъобразността на обработването на личните данни ще зависи от целта на това обработване[119]. Целта трябва да бъде определена и оповестена от администратора преди да започне обработването на данните[120]. **Съгласно правото на ЕС** това трябва да бъде изпълнено или чрез декларация, или с други думи чрез уведомление до съответния надзорен орган, или най-малкото чрез вътрешна документация, която администраторът трябва да предостави на разположение за проверка от надзорните органи и за достъп от страна на съответното физическо лице.

Обработването на личните данни за неопределени и/или неограничени цели е незаконосъобразно.

Всяка нова цел за обработване на данните трябва да има свое собствено конкретно правно основание и не може да се основава на факта, че данните

119 Конвенция № 108, член 5, буква б); Директива за защита на личните данни, член 6, параграф 1, буква б).

120 Вж. също Работна група за защита на личните данни по член 29 (2013 г.), *Opinion 03/2013 on purpose limitation [Становище 03/2013 относно ограничаването на целта]*, WP 203, Брюксел, 2 април 2013 г.

са били първоначално получени или обработени с друга законна цел. От своя страна законосъобразното обработване е ограничено до първоначално определената си цел и всяка нова цел на обработването изисква отделно ново правно основание. Разкриването на данни на трети лица трябва да бъде обмислено особено внимателно, тъй като то обикновено представлява нова цел и следователно изисква правно основание, различно от основанието за събирането на данните.

Пример: Авиокомпания събира данни от своите пътници, за да направи резервации, с цел правилното осъществяване на полета. Авиокомпанията се нуждае от данни за: номерата на местата на пътниците, специалните физически ограничения, като например необходимостта от инвалидни колички, и специалните изисквания по отношение на храната, като например кошер или халал. Ако към авиокомпаниите бъде отправено искане да осъществят трансфер на данните, които се съдържат в резервационните данни на пътниците (PNR), на имиграционните органи на летището при приземяването, тогава тези данни се използват за целите на имиграционния контрол, които са различни от първоначалната цел за събиране на данните. Трансферът на тези данни към имиграционните органи следователно ще изисква ново и отделно правно основание.

Когато се разглеждат обхватът и ограниченията на конкретна цел, в Конвенция № 108 и Директивата за защита на личните данни се прибягва до понятието за съвместимост: използването на данни за съвместими цели е разрешено въз основа на първоначалното правно основание. Какво означава „съвместими“ обаче не е определено и остава отворено за тълкуване въз основа на всеки отделен случай.

Пример: Продажбата на данните на клиентите на дружество Sunshine, придобити от дружеството в хода на управлението на връзките с клиенти (CRM данните), на дружество за директен маркетинг, Moonlight, което иска да използва тези данни за подпомагане на маркетинговите кампании на трети дружества, е нова цел, която е несъвместима с управлението на връзките с клиенти — първоначалната цел на дружество Sunshine, за която са били събрани данните на клиентите. Продажбата на данните на дружество Moonlight следователно се нуждае от свое собствено правно основание.

За разлика от това, използването от дружество Sunshine на CRM данните за негови собствени маркетингови цели, т.е. изпращането на маркетингови съобщения до собствени клиенти за собствени продукти на дружеството, по принцип се приема за съвместима цел.

В Директивата за защита на личните данни изрично се заявява, че „допълнителната обработка на данните за исторически, статистически или научни цели няма да се разглежда като несъвместима, при условие че държавите членки предоставят необходимите гаранции за това“[121].

Примери: Дружество Sunshine е събрало и съхранявало CRM данни за своите клиенти. По-нататъшното използване на тези данни от дружество Sunshine за статистически анализ на поведението на неговите клиенти по отношение на закупуването на стоки е допустимо, тъй като статистиката е съвместима цел. Не се изисква допълнително правно основание, като например съгласието на физическите лица.

Ако същите данни би трябвало да бъдат предадени на трето лице — на дружество Starlight — единствено за статистически цели, предаването би било допустимо без допълнително правно основание, но само при условие че са налични съответните гаранции, като например скриване на самоличността на съответните физически лица, тъй като самоличността обикновено не е необходима за статистически цели.

3.3. Принципи за качество на данните

Ключови въпроси

- Принципите за качество на данните трябва да бъдат прилагани от администратора във всички операции по обработването.
- Принципът за ограничен период на запазване на данни налага изтриването на данните в момента, в който те вече не са необходими за целите, за които са били събрани.

121 Пример за такива национални разпоредби е австрийският Закон за защита на данните (*Datenschutzgesetz*), Fed. Law Gazette (Федерален държавен вестник) I № 165/1999, точка 46, достъпен на английски език на адрес: www.dsk.gv.at/DocView.axd?CobId=41936.

- Освобождаването от принципа за лимитиран период на запазване на данни трябва да бъде определено от закона и изисква специални гаранции за защитата на физическите лица.

3.3.1. Принципът за съотносимост на данните

Обработват се само такива данни, които са „адекватни, релевантни, и [...] не са прекомерни по отношение на целите, за които се събират и/или обработват допълнително“[122]. Категориите на избраните данни за обработване трябва да бъдат необходими за постигане на обявената обща цел на операциите по обработването, а администраторът следва стриктно да ограничава събирането на данните до такава информация, която е директно свързана с конкретната цел на обработването.

В съвременното общество принципът за съотносимост на данните има допълнително значение: чрез използването на специална технология за подобряване на неприкосновеността на личния живот понякога е възможно въобще да се избегне използването на лични данни или да се използват данни под псевдоним, което води до решение, благоприятстващо защитата на данните. Това е особено подходящо в по-широкообхватни системи за обработване на данни.

Пример: Градският съвет предлага карта с чип за редовните потребители на градската обществена транспортна система срещу определена такса. Върху картата е изписано името на потребителя, като то се съдържа също и в електронна форма в чипа. Винаги когато се използва автобус или трамвай, картата с чип трябва да бъде поставена пред монтираните четящи устройства, например в автобуси и трамваи. Данните, прочетени от устройството, се проверяват електронно в база данни, съдържаща имената на хората, които са закупили карта за пътуване.

Тази система не спазва по оптимален начин принципа за съотносимост на данните: проверката на това дали на дадено лице е разрешено да използва транспортната система може да се извърши без да се сравняват личните данни в чипа на картата с база данни. Например би било достатъчно наличието на специален електронен образ, като например бар код, в чипа на картата, който при поставяне пред четящото устройство

122 Конвенция № 108, член 5, буква в) и Директива за защита на личните данни, член 6, параграф 1, буква в).

би потвърдил дали картата е валидна или не. Такава система няма да записва кой е използвал дадено транспортно средство и по кое време. Няма да се събират лични данни, което е оптимално решение по смисъла на принципа за съотносимост, тъй като този принцип спазвазадължението събирането на данни да бъде сведено до минимум.

3.3.2. Принципът за точност на данните

Администратор, който съхранява лични данни, не трябва да ги използва преди да е придприел необходимите стъпки, за гарантиране на тяхната точност и актуалност. Задължението за гарантиране на точността на данните трябва да бъде разглеждано в зависимост от целта за обработване на данните.

Пример: Дружество за продажба на мебели е събрало данни за самоличността и адреса на клиент, за да му издаде фактура. Шест месеца по-късно същото дружество иска да започне маркетингова кампания и желае да се свърже с предишни свои клиенти. За да се свърже с тях, дружеството иска достъп до националния регистър на гражданите, в който вероятно се съдържат актуални адреси, тъй като гражданите са задължени по закон да регистрират в регистъра текущите си адреси. Достъпът до данните в този регистър е ограничен до физически и юридически лица, които могат да представят основателна причина.

При това положение дружеството не може да използва довода, че данните трябва да се поддържат точни и актуални, за да докаже, че има право да събира данни за новите адреси на всички свои предишни клиенти от регистъра на гражданите. Данните са били събрани в хода на фактурирането; за тази цел отношение има адресът в момента на продажбата. Не е налице правно основание за събиране на данни за нови адреси, тъй като маркетингът не е интерес, който има преимущество над правото за защита на данните и следователно не може да обоснове достъпа до данните в регистъра.

Също така може да има случаи, при които актуализирането на съхранените данни е забранено от закона, тъй като целта на съхраняването на данните принципно се състои в документирането на събития.

Пример: Протокол от медицинска операция не трябва да бъде променян, с други думи, „актуализиран“, дори ако по-късно се окаже, че посочените в протокола констатации са били погрешни. При такива обстоятелства могат да бъдат направени само допълнения към бележките в протокола, стига да са ясно отбелязани като допълнения, направени на по-късен етап.

От друга страна, има ситуации, при които редовните проверки на точността на данните, включително актуализирането, са абсолютно необходими поради потенциалната вреда, която може да бъде нанесена на съответното физическо лице, ако данните останат неточни.

Пример: Ако някой иска да сключи договор с банкова институция, банката обикновено проверява кредитоспособността на бъдещия клиент. За тази цел на разположение е специални бази данни, съдържаща данни за кредитната история на частни лица. Ако такава база данни предоставя неточни или неактуални данни за дадено лице, това лице може да срещне сериозни проблеми. Администраторите на такива бази данни следователно трябва да положат специални усилия за спазване на принципа за точност на данните.

Освен това данните, които не са свързани с факти, а с подозрения, като например с наказателни разследвания, могат да бъдат събирани и съхранявани дотогава, докато администраторът има правно основание да събира такива данни и има достатъчно основателна причина за подобно подозрение.

3.3.3. Принципът за ограничен период на запазване на данни

Член 6, параграф 1, буква д) от Директивата за защита на личните данни, а също така член 5, буква д) от Конвенция № 108, изискват от държавите членки да гарантират, че личните данни „се поддържат във форма, която позволява идентифицирането на съответните физически лица за срок не по-дълъг от необходимия за целите, за които тези данни са събрани или обработени допълнително“. Следователно данните трябва да бъдат изтрити, когато тези цели бъдат изпълнени.

По делото *S. и Marper* ЕСПЧ е заключил, че основните принципи на съответните инструменти на Съвета на Европа и законодателството и практиката на

другите договарящи се страни изискват запазването на данни да бъде пропорционално по отношение на целта, за която данните са събрани, и да бъде ограничено във времето, особено в сектора на полицията[123].

Времевото ограничение за съхраняването на лични данни обаче е приложимо само за данни, съхранявани във форма, която позволява идентифицирането на съответните физическите лица. Следователно законосъобразното съхраняване на данни, които вече не са необходими, би могло да бъде постигнато чрез анонимизиране на данните или представяне на данните чрез използване на псевдоним.

Запазването на данните за бъдещо използване за исторически, статистически или научни цели е изрично освободено от принципа за ограничения период на запазване на данни в Директивата за защита на личните данни[124]. Подобно текущо съхраняване и използване на лични данни, обаче, трябва да бъде придружено от специални гаранции съгласно националното законодателство.

3.4. Принципът за добросъвестно обработване на данните

Ключови въпроси

- Добросъвестното обработване означава прозрачност на обработването, особено по отношение на физическите лица.
- Администраторите трябва да информират съответните физически лица преди да обработват техните данни поне относно целта на обработването и относно самоличността и адреса на администратора.
- Освен ако не е специално позволено от закона, не трябва да има тайно и скрито обработване на лични данни.
- Съответните физически лица имат право на достъп до своите данни във всички случаи, в които те биват обработвани.

123 ЕСПЧ, Решение от 4 декември 2008 г. по дело *S. и Marper/Обединеното кралство*, № 30562/04 и 30566/04; вж. също например ЕСПЧ, Решение от 13 ноември 2012 г по дело *М.М./Обединеното кралство*, № 24029/07.

124 Директива за защита на личните данни, член 6, параграф 1, буква д).

Принципът за добросъвестно обработване регламентира предимно взаимоотношенията между администратора и физическото лице.

3.4.1. Прозрачност

Този принцип установява задължение за администратора да информира физическите лица относно това как се използват техните данни.

> Пример: В делото *Haralambie/Румъния*[125] жалбоподателят е искал достъп до досието, което секретната служба е съхранявала за него, но искането му е било удовлетворено едва пет години по-късно. ЕСПЧ отново е заявил, че лицата с лични досиета, съхранявани от обществени органи, са имали жизненоважен интерес да разполагат с възможност за достъп до тези досиета. Органите са имали задължение да осигурят ефективна процедура за получаване на достъп до такава информация. ЕСПЧ е счел, че нито количеството на прехвърлените досиета, нито недостатъците в системата за архивиране оправдават забавянето от пет години да се удовлетвори искането на жалбоподателя за достъп до неговото досие. Органите не са осигурили ефективна и достъпна процедура за жалбоподателя, за да му дадат възможност да получи достъп до неговото лично досие в разумен срок. Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

Операциите по обработването трябва да бъдат обяснени на физическите лица по лесно достъпен начин, който да гарантира, че те разбират какво ще се случи с данните им. Съответното физическо лице също така има право при поискване да бъде информирано от администратора относно това, дали се обработват негови данни и ако да — кои данни се обработват.

3.4.2. Създаване на доверие

Администраторите следва документално да докажат на съответните физически лица и на широката общественост, че ще обработват данните по законосъобразен и прозрачен начин. Операциите по обработването не трябва да бъдат извършвани тайно и не следва да имат непредвидими отрицателни последици. Администраторите следва да гарантират, че клиентите или гражданите са информирани относно използването на техните данни. Освен това

125 ЕСПЧ, Решение от 27 октомври 2009 г. по дело *Haralambie /Румъния*, № 21737/03.

администраторите, доколкото е възможно, трябва да действат по начин, който точно да съответства на желанията на физическото лице, особено когато неговото съгласие представлява правното основание за обработването на данните.

Пример: В делото *K.H и други/Словакия*[126] жалбоподателките са осем жени от ромски произход, които са били на лечение в две болници в Източна Словакия по време на бременност и раждане. След това нито една от тях не е успяла отново да зачене дете въпреки неднократните опити. Националните съдилища са издали нареждане на болниците да разрешат на жалбоподателките и представляващите ги лица да разгледат и направят писмени извадки от медицинските документи, но са отхвърлили искането им да фотокопират документите с твърдението, че това е с цел да се предотврати злоупотреба с тях. Положителните задължения на държавите съгласно член 8 от ЕКПЧ непременно включват задължение на физическите лица да бъдат предоставяни копия от техните досиета с данни. Държавата е тази, която е трябвало да определи условията за копиране на досиетата с лични данни или, когато е уместно, да представи убедителни причини за отказа да се извърши това. В случая на жалбоподателките националните съдилища са обосновали забраната за изготвяне на копия на медицинските документи главно чрез необходимостта да се защити съответната информация от злоупотреба. ЕСПЧ обаче не е счел, че жалбоподателките, които при всички случаи са имали достъп до пълните медицински досиета, биха могли да злоупотребят с информация, касаеща тях самите. Освен това рискът от такава злоупотреба е било възможно да бъде предотвратен по начин, различен от отказа на жалбоподателките да направят копия на досиетата, например чрез ограничаване на броя на лицата, имащи право на достъп до досиетата. Държавата не е успяла да докаже съществуването на достатъчно убедителни причини на жалбоподателките да бъде отказан ефективен достъп до информация, касаеща тяхното здраве. Съдът е заключил, че е налице нарушение на член 8.

По отношение на интернет услугите функционалностите на системите за обработване на данни трябва да направят възможно физическите лица действително да разбират какво се случва с техните данни.

126 ЕСПЧ, Решение от 6 ноември 2009 г. по дело *K.H и други/Словакия*, № 32881/04.

Добросъвестното обработване също така означава, че администраторите имат готовност да надхвърлят задължителните минимални правни изисквания за обслужване на съответното физическо лице, ако законните му интереси налагат това.

3.5. Принципът за отчетност

Ключови въпроси

- Отчетността изисква администраторите активно да прилагат мерки за насърчаване и гарантиране на защитата на данните в своите дейности по обработване.
- Администраторите носят отговорност за съответствието на своите операции по обработване с правото зазащитата на данните.
- Администраторите следва да бъдат в състояние по всяко време да докажат пред физическите лица, обществеността и надзорните органи своето съответствие с разпоредбите за защита на данните.

През 2013 г. Организацията за икономическо сътрудничество и развитие (ОИСР) прие Насоки относно защитата на неприкосновеността на личния живот, в които подчертава, че администраторите играят важна роля за практическото приложение на защитата на данните. В насоките е развит принципът за отчетност, съгласно който „администраторът на данни следва да бъде отговорен за спазване на мерките, които пораждат действие по отношение на [материалните] принципи, посочени по-горе“[127].

Докато в Конвенция № 108 не се посочва отчетността на администраторите, а оставя този въпрос на националното законодателство, член 6, параграф 2 от Директивата за защита на личните данни гласи, че администраторът следва да осигурява спазването на принципите, отнасящи се до качеството на данните, посочени в параграф 1.

127 (ОИСР) (2013 г.) *Насоки, уреждащи защитата на неприкосновеността на личния живот и трансграничните потоци от лични данни*, член 14.

Пример: Законодателен пример, подчертаващ принципа за отчетност, е изменението от 2009 г.[128] на Директивата за правото на неприкосновеност на личния живот и електронни комуникации — Директива 2002/58/ЕО. В член 4, в своя изменен вид, директивата налага задължение за прилагане на политика на сигурност, по-специално, за да се гарантира „осъществяването на политика на сигурност по отношение на обработката на лични данни". По такъв начин, що се отнася до предвидените в тази директива разпоредби за сигурност, законодателят е решил, че е необходимо да се въведе изрично изискване за наличието и осъществяването на политика на сигурност.

Съгласно становището на Работната група по член 29[129] същността на отчетността се състои в задължението на администратора да:

- въведе мерки, които при нормални обстоятелства ще гарантират, че правилата за защита на данните се спазват при извършване на операции по обработване; и

- разполага с готова документация, която доказва на физическите лица и на надзорните органи какви мерки са взети за спазване на правилата за защита на данните.

По този начин принципът за отчетност изисква от администраторите да докажат активното спазване на правилата, а не просто да чакат физическите лица или надзорните органи да посочват недостатъци.

128 Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите, ОВ L 337, 18.12.2009 г., стр. 11.

129 Работна група за защита на личните данни по член 29, *Становище 3/2010 относно принципа на отчетността*, WP 173, Брюксел, 13 юли 2011 г.

4

Правилата на европейското право в областта на защитата на данните

ЕС	Обхванати въпроси	Съвет на Европа
Правила относно законосъобразното обработване на нечувствителни данни		
Директива за защита на личните данни, член 7, буква а)	**Съгласие**	Препоръка относно профилирането, член 3.4, буква б) и член 3.6
Директива за защита на личните данни, член 7, буква б)	**(Преддоговорни) Договорни отношения**	Препоръка относно профилирането, член 3.4, буква б)
Директива за защита на личните данни, член 7, буква в)	**Правни задължения на администратора**	Препоръка относно профилирането, член 3.4, буква а)
Директива за защита на личните данни, член 7, буква г)	**Жизненоважни интереси на съответното физическо лице**	Препоръка относно профилирането, член 3.4, буква б)
Директива за защита на личните данни, член 7, буква д) и член 8, параграф 4 Съд на ЕС, Решение от 16 декември 2008 г. по дело *Huber/Германия*, C-524/06	**Обществения интерес и упражняването на официални правомощия**	Препоръка относно профилирането, член 3.4, буква б)
Директива за защита на личните данни, член 7, параграф. еи член 8, параграфи 2 и 3 Съд на ЕС, Решение от 24 ноември 2011 г. по съединени дела *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) u Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10)/Administración del Estado*, C-468/10 и C-469/10	**Законни интереси на други лица**	Препоръка относно профилирането, член 3.4, буква б)

Правила относно законосъобразното обработване на чувствителни данни		
Директива за защита на личните данни, член 8, параграф 1	**Обща забрана за обработване**	Конвенция № 108, член 6
Директива за защита на личните данни, член 8, параграфи 2—4	**Изключения от общата забрана за обработване**	Конвенция № 108, член 6
Директива за защита на личните данни, член 8, параграф 5	**Обработване на данни, отнасящи се до (наказателни) присъди**	Конвенция № 108, член 6
Директива за защита на личните данни, член 8, параграф 7	**Обработване на идентификационни номера**	
Правила относно сигурността на обработването		
Директива за защита на личните данни, член 17	**Задължение за осигуряване на сигурност на обработването**	Конвенция № 108, член 7
		ЕСПЧ, Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03
Директива за правото на неприкосновеност на личния живот и електронни комуникации, член 4, параграф 2	**Уведомления за нарушения на сигурността на данните**	
Директива за защита на личните данни, член 16	**Задължение за поверителност**	
Правила за прозрачност при обработването		
	Прозрачността по принцип	Конвенция № 108, член 8, буква а)
Директива за защита на личните данни, членове 10 и 11	**Информация**	Конвенция № 108, член 8, буква а)
Директива за защита на личните данни, членове 10 и 11	**Изключения от задължението за информиране**	Конвенция № 108, член 9
Директива за защита на личните данни, членове 18 и 19	**Уведомяване**	Препоръка относно профилирането, член 9.2, буква а)
Правила относно насърчаване на спазването на разпоредбите		
Директива за защита на личните данни, член 20	**Предварителна проверка**	
Директива за защита на личните данни, член 18, параграф 2	**Длъжностни лица за защита на личните данни**	Препоръка относно профилирането, член 8.3
Директива за защита на личните данни, член 27	**Кодекси за поведение**	

Необходимо е принципите да са с общ характер. Тяхното прилагане в конкретни ситуации оставя известна свобода за тълкуване и избор на средства. Правото на **Съвета на Европа** оставя на страните по Конвенция № 108 да изяснят тази свобода на тълкуване в националното си законодателство. Положението в **правото на ЕС** е различно: по отношение на установяването на защита на данните във вътрешния пазар беше счетено, че е необходимо да има вече въведени по-подробни правила на равнище ЕС, за да се хармонизира нивото на защита на данните в националните законодателства на държавите членки. Директивата за защита на личните данни определя, следвайки принципите, посочени в член 6 от нея, набор от подробни правила, които трябва да бъдат надлежно въведени в националното законодателство. Поради тази причина следващите коментари относно подробните правила за защита на данните на европейско равнище се отнасят предимно до правото на ЕС.

4.1. Правила за законосъобразно обработване

Ключови въпроси

- Лични данни могат да бъдат законосъобразно обработвани, ако:
  - обработването се основава на съгласието на съответното физическо лице; или
  - жизненоважни интереси на съответните физически лица изискват обработването на техните данни; или
  - законни интереси на други лица са основанието за обработването, но само ако спрямо тях нямат преимущество интереси, свързани със защитата на основните права на съответните физически лица.
- Законосъобразното обработване на чувствителни лични данни подлежи на специален, по-строг режим.

Директивата за защита на личните данни съдържа два различни набора от правила за законосъобразно обработване на данни: един за нечувствителни данни — в член 7, и друг за чувствителни данни — в член 8.

4.1.1. Законосъобразно обработване на нечувствителни данни

В глава II от Директива 95/46/ЕО, озаглавена „Общи правила относно законността на обработването на лични данни“ се предвижда, че при спазване на изключенията, разрешени съгласно член 13, всяко обработване на лични данни трябва да отговаря първо на принципите, отнасящи се до качеството на данните, посочени в член 6 от Директивата за защита на личните данни, и второ — на един от критериите за законосъобразност на обработването на данни, посочени в член 7[130]. Това обяснява случаите, в които обработването на нечувствителни лични данни е законосъобразно.

Съгласие

Съгласно правото на Съвета на Европа съгласието не се посочва в член 8 от ЕКПЧ или в Конвенция № 108. То обаче се споменава в съдебната практика на ЕСПЧ и в няколко препоръки на Съвета на Европа. **Съгласно правото на ЕС** съгласието като основание за законосъобразното обработване на данните е твърдо установено в член 7, параграф а) от Директивата за защита на личните данни и също така изрично е посочено в член 8 от Хартата.

Договорни отношения

Друго основание за законосъобразното обработване на лични данни **съгласно правото на ЕС**, посочено в член 7, буква б) от Директивата за защита на личните данни, е ако то е „необходимо за изпълнението на договор, по който съответното физическо лице е страна“. Тази разпоредба обхваща и преддоговорните отношения. Например: една страна възнамерява да сключи договор, но все още не го е направила, вероятно защото все още трябва да бъдат приключени някои проверки. Ако едната страна трябва да обработи данни за тази цел, това обработване е законосъобразно, ако то се извършва, „за да се предприемат стъпки по искане на съответното физическо лице преди сключването на договора“.

130 Съд на ЕС, Решение от 20 май 2003 г. по съединени дела *Österreichischer Rundfunk и други*, C-465/00, C-138/01 и C-139/01, точка 65; Съд на ЕС, Решение от 16 декември 2008 г. по дело *Huber/Bundesrepublik Deutschland*, C-524/06, точка 48; Решение от 24 ноември 2011 г. по съединени дела *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) u Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10)/Administración del Estado*, съединени дела C-468/10 и C-469/10, точка 26.

Що се отнася до правото на Съвета на Европа, „защитата на [...] правата и свободите на другите“ е посочена в член 8, параграф 2 от ЕКПЧ като основание за законна намеса в правото на защита на данните.

Правни задължения на администратора

Освен това в **правото на ЕС** изрично се посочва друг критерий за законосъобразност на обработването на данни, а именно, ако то „е необходимо за спазването на правно задължение, чийто субект е администраторът“ (член 7, буква в) от Директивата за защита на личните данни). Тази разпоредба се отнася до администраторите в частния сектор; правните задължения на администраторите на данни в публичния сектор попадат в обхвата на член 7, буква д) от директивата. Има много случаи, в които администраторите в частния сектор са законово задължени да обработват данни за други лица; например лекарите и болниците са законово задължени да съхраняват данни относно лечението на пациенти в продължение на няколко години, работодателите трябва да обработват данни за своите служители по причини, свързани със социалната сигурност и данъчното облагане, а предприятията трябва да обработват данни за своите клиенти по причини, свързани с данъчното облагане.

Във връзка със задължителния трансфер на данни на пътниците, който се извършва от авиокомпаниите до имиграционните контролни органи на чужди държави, възникна въпросът дали законови задължения съгласно *чуждестранно* право биха могли да представляват основание за законосъобразно обработване на данни съгласно правото на ЕС (този въпрос е разгледан по-подробно в раздел 6.2).

Правните задължения на администратора служат като основание за законосъобразно обработване на данни и **съгласно правото на Съвета на Европа**. Както беше посочено по-горе, правните задължения на администратор в частния сектор са само един конкретен случай за законни интереси на други лица, както е посочено в член 8, параграф 2 от ЕКПЧ. Поради тази причина, горепосоченият пример се отнася и за правото на Съвета на Европа.

Жизненоважни интереси на съответното физическо лице

Съгласно правото на ЕС в член 7, буква г) от **Директивата за защита на личните данни** се предвижда, че обработването на лични данни е законосъобразно,

ако то „е необходимо, за да бъдат защитени жизнено важни интереси на съответното физическо лице“. Такива интереси, които са тясно свързани с оцеляването на съответното физическо лице, могат да бъдат основание за законно използване например на здравни данни или на данни за изчезнали лица.

Съгласно правото на Съвета на Европа жизненоважните интереси на съответното физическо лице не се посочват в член 8 от ЕКПЧ като основание за законна намеса в правото на защита на данните. В някои от препоръките на Съвета на Европа, които допълват Конвенция № 108 в конкретни области, жизненоважните интереси на съответното физическо лице обаче са изрично посочени като основание за законосъобразно обработване на данни[131]. По отношение на жизненоважните интереси на съответното физическо лице очевидно се счита, че те се подразбират в набора от основания, обосноваващи обработването на данни: защитата на основните права не следва никога да застрашава жизненоважните интереси на защитаваното лице.

Обществен интерес и упражняване на официални правомощия

С оглед на множеството възможни начини за организиране на публичните дела в член 7, буква д) от **Директивата за защита на личните данни** се предвижда, че личните данни могат да бъдат обработвани законосъобразно, ако обработването „е необходимо за изпълнението на задача, която се осъществява в обществен интерес или при упражняване на официалните правомощия, които са предоставени на администратора или трето лице, на което се разкриват данните [...] »[132]

Пример: В делото *Huber/Германия*[133] г-н Huber, пребиваващ в Германия, австрийски гражданин, е поискал от Федералната служба за миграцията и бежанците заличаване на свързани с него данни в Централния регистър за чужденците (наричан по-нататък „AZR“). Регистърът, който съдържа лични данни за граждани на ЕС, които не са германски граждани, но пребивават в Германия в продължение на повече от три месеца, се използва за статистически цели, както и от правоприлагащите и съдебните органи при разследването и наказателното преследване на престъпни дейности или на такива, които представляват заплаха за обществената сигурност.

131 Препоръка относно профилирането, член 3.4, буква б).

132 Вж. също Директива за защита на личните данни, съображение 32

133 Съд на ЕС, Решение от 16 декември 2008 г. по дело *Huber/Bundesrepublik Deutschland*, C-524/06.

Препращащият съд е отправил запитване дали обработването на лични данни, извършвано в регистър като Централния регистър за чужденците, до който други публични органи също имат достъп, е съвместимо с правото на ЕС, като се има предвид, че не съществува такъв регистър за германските граждани.

Съдът на ЕС на първо място е констатирал, че съгласно член 7, буква д) от директивата личните данни могат да бъдат обработвани законосъобразно само ако обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес или при упражняване на официални правомощия.

Според Съда „предвид целта да се осигури еднаква степен на защита във всички държави членки понятието за необходимост, което произтича от член 7, буква д) от Директива 95/46, [...] не може да има различно съдържание в зависимост от държавите членки. Следователно става въпрос за самостоятелно понятие на общностното право, на което трябва да се направи тълкуване, отговарящо в пълна степен на предмета на тази директива, определен в член 1, параграф 1 от нея“[134].

Съдът отбелязва, че правото на свободно движение на гражданин на Съюза на територията на държава членка, на която не е гражданин, не е безусловно, а може да бъде придружено с ограничения и условия, предвидени от Договора, както и от разпоредбите, приети за неговото прилагане. Следователно ако използването на регистър като AZR, за да се подпомагат органите, отговарящи за прилагането на нормативната уредба относно правото на пребиваване, по принцип е законосъобразно за дадена държава членка, то този регистър трябва да съдържа само необходимата за тази цел информация. Съдът заключва, че такава система за обработване на лични данни е в съответствие с правото на ЕС, ако тя съдържа единствено данните, които са необходими, за да се прилага тази нормативна уредба, и ако централизираният характер позволява по-ефективното прилагане на тази нормативна уредба. Националната юрисдикция трябва да провери дали в конкретния случай тези условия са изпълнени. Ако не са, при всяко положение съхранението и обработването на лични данни в рамките на регистър като AZR за статистически

134 *Пак там*, точка 52.

цели не могат да се приемат за необходими по смисъла на член 7, буква д) от Директива 95/46/ЕО[135].

Накрая, що се отнася до въпроса за използването на съдържащите се в регистъра данни с цел борба с престъпността, Съдът счита, че тази цел „със сигурност е да се преследват извършените престъпления и деликти без оглед на гражданството на извършителя им". Въпросният регистър не съдържа лични данни, отнасящи се до граждани на съответната държава членка, и това различно третиране представлява дискриминация, забранена от член 18 от ДФЕС. Следователно тази разпоредба, съгласно даденото от Съда тълкуване, „не допуска с оглед на целта за борба с престъпността държава членка да създаде система за обработване на лични данни специално за гражданите на Съюза, които не са граждани на тази държава членка"[136].

Използването на лични данни от органи в публичната сфера също влиза в обхвата на разпоредбите на член 8 от **ЕКПЧ**.

Законни интереси, преследвани от администратора или от трето лице

Съответното физическо лице не е единственото със законни интереси. Член 7, буква е) от **Директивата за защита на личните данни** предвижда, че личните данни могат да бъдат обработвани законосъобразно ако обработването „е необходимо за целите на законните интереси, преследвани от администратора или от трето лице или лица, на които се разкриват данните, с изключение на случаите, когато пред тези интереси имат преимущество интереси, свързани с основните права и свободи на съответното физическо лице, които изискват защита [...]".

В следното решение Съдът на ЕС отсъди изрично въз основа на член 7, буква е) от директивата:

Пример: В решението по дело *ASNEF и FECEMD*[137] Съдът на ЕС поясни, че не е разрешено в националното законодателство да се добавят условия

135 *Пак там*, точки 54, 58, 59, 66–68.

136 *Пак там*, точки 78 и 81.

137 Съд на ЕС, Решение от 24 ноември 2011 г. по съединени дела *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) u Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10)/Administración del Estado*, съединени дела C-468/10 и C-469/10.

в допълнение към тези, посочени в член 7, буква е) от Директивата, за законосъобразно обработване на данни. Това се отнасяше за ситуация, при която в испанското законодателство за защита на данните се е съдържала разпоредба, съгласно която други частни лица са можели да предявят законен интерес за обработването на лични данни само ако информацията вече е била оповестена в публични източници.

Съдът първо отбеляза, че Директива 95/46/ЕО има за цел да уеднакви във всички държави членки степента на защита на правата и свободите на лицата при обработването на лични данни. Освен това сближаването на приложимите в тази област национални законодателства не трябва да доведе до намаляване на степента на защита, която те осигуряват, а всъщност то трябва да има за цел гарантиране на висока степен на защита в Съюза[138]. При това положение, Съдът на ЕС постанови, че „от целта да се осигури еднаква степен на защита във всички държави членки следва, че член 7 от Директива 95/46 съдържа изчерпателен списък на случаите, в които обработването на лични данни може да се счита за законно". Освен това „държавите членки не могат нито да добавят нови критерии за законност на обработването на лични данни към член 7 от Директива 95/46, нито да предвиждат допълнителни изисквания, които изменят обхвата на някой от шестте критерия, посочените в този член"[139]. Съдът допусна, че „във връзка с необходимото търсене на баланс, съгласно член 7, буква е) от Директива 95/46, е възможно да се вземе предвид обстоятелството, че тежестта на засягане на основните права на лицето, до което се отнасят съответните данни, може да е различна в зависимост от това,дали тези данни се съдържат или не в общодостъпни източници".

Обаче „член 7, буква е) от тази директива не допуска държава членка да изключи категорично и безусловно възможността за обработване на някои категории лични данни, без да извърши преценка във всеки конкретен случай на съответните противоположни права и интереси".

138 *Пак там*, точка 28. Вж. Директива за защита на личните данни, съображения 8 и 10.

139 Съд на ЕС, Решение от 24 ноември 2011 г. по съединени дела *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) u Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10)/Administración del Estado*, съединени дела C-468/10 и C-469/10, точки 30 и 32.

> С оглед на тези съображения Съдът заключи, че „член 7, буква е) от Директива 95/46/ЕО [...] трябва да се тълкува в смисъл, че не допуска национална правна уредба, която при отсъствие на съгласие на физическото лице и с оглед разрешаването на обработването на лични данни поради наличие на законен интерес на администратора или на едно или повече трети лица, изисква не само спазването на основните права и свободи на субектите на данни, но и наличието на тези данни в общндостъпни източници , като по този начин изключва категорично и безусловно обработването на данни, които не се съдържат в такива източници“[140].

Подобни формулировки могат да бъдат намерени в **препоръките на Съвета на Европа**. В Препоръката относно профилирането се признава като законно обработването на лични данни за целите на профилиране, ако то е необходимо за законните интереси на други лица, „с изключение на случаите, когато пред тези интереси имат преимущество интереси, свързани с основните права и свободи на съответното физическо лице“[141].

4.1.2. Законосъобразно обработване на чувствителни данни

Правото на Съвета на Европа оставя на националното законодателство да определи подходяща защита при използването на чувствителни данни, докато **правото на ЕС**, в член 8 от Директивата за защита на личните данни, съдържа подробен режим за обработването на категории данни, които разкриват: расов или етнически произход, политически идеи, религиозни или философски убеждения, членство в професионални съюзи или данни, свързани със здравословното състояние или половия живот. Обработването на чувствителни данни по принцип е забранено[142]. Съществува обаче изчерпателен списък с посочени изключения от тази забрана, който може да бъде намерен в член 8, параграфи 2 и 3 от директивата. Тези изключения включват изричното съгласие на физическото лице, неговите жизненоважни интереси, законните интереси на други лица и обществения интерес.

За разлика от случая с обработването на нечувствителни данни, наличието на договорно отношение с физическото лице не се счита за общо основание

140 *Пак там*, точки 40, 44, 48 и 49.

141 Препоръка относно профилирането, член 3.4, буква б).

142 Директива за защита на личните данни, член 8, параграф 1.

за законосъобразното обработване на чувствителни данни. Следователно, ако чувствителни данни трябва да бъдат обработени за изпълнение на договор с физическото лице, използване на тези данни изисква това лице да даде отделно изрично съгласие в допълнение към съгласието за сключване на договора. Изрично искане от страна на физическото лице на стоки или услуги, при предоставянето на които непременно се разкриват чувствителни данни, следва обаче да се счита за равностойно на даването на изрично съгласие.

Пример: Ако пътуващ с дадена авиокомпания, във връзка с извършването на резервация за полет, изиска от авиокомпанията да му осигури инвалидна количка и храна тип „кошер", на авиокомпанията е позволено да използва тези данни, дори ако пътникът не е подписал допълнителна клауза за съгласие, в която се посочва, че е съгласен да се използват негови данни, разкриващи информация за здравословното му състояние и религиозните му убеждения.

Изрично съгласие на физическото лице

Първото условие за законосъобразно обработване на данни, независимо от това дали те са нечувствителни или чувствителни данни, е съгласието на физическото лице. По отношение на чувствителните данни това съгласие трябва да бъде изрично. В националното законодателство може обаче да се предвижда, че даването на съгласие за използването на чувствителни данни не е достатъчно правно основание за разрешаване на тяхното обработване[143], например когато в изключителни случаи обработването включва необичайни рискове за съответното физическо лице.

В един специален случай, дори мълчаливото съгласие се признава за правно основание за обработването на чувствителни данни: В член 8, параграф 2, буква д) от директивата се предвижда, че обработването не е забранено, ако то е свързано с данни, които явно са направени публично достояние от съответното физическо лице. Тази разпоредба очевидно предполага, че действието на съответното физическо лице, с което то прави своите данни публично достояние, трябва да се тълкува като даване на неговото съгласие за използването на тези данни.

143 *Пак там*, член 8, параграф 2, буква а).

Жизненоважни интереси на съответното физическо лице

Както при нечувствителните данни, чувствителните данни могат да бъдат обработвани поради основания, свързани с жизненоважните интереси на съответното физическо лице[144].

За да бъде обработването на чувствителни данни законно на това основание, е необходимо да е невъзможно от съответното физическо лице да бъде поискано да вземе такова решение, например поради това, че то е в безсъзнание или отсъства и не може да бъде установена връзка с него.

Законни интереси на други лица

Както и при нечувствителните данни, законните интереси на други лица могат да служат като основание за обработването на чувствителни данни. За чувствителни данни и съгласно член 8, параграф 2 от Директивата за защита на личните данни, това обаче, се прилага само в следните случаи:

- ако обработването е необходимо за защита на жизненоважните интереси на друго лице[145], когато съответното физическо лице е физически или юридически неспособно да даде своето съгласие;

- когато чувствителни данни са приложими в областта на трудовото право, като например здравни данни — например във връзка с особено опасно работно място, или данни относно религиозни убеждения — например във връзка с празници[146];

- когато фондации, сдружения или други организации с нестопанска цел, с политическа, философска, религиозна или профсъюзна цел, обработват данни относно техните членове или спонсори, или други заинтересовани лица (тези данни са чувствителни, тъй като те вероятно разкриват религиозните или политическите убеждения на съответните лица)[147];

144 *Пак там*, член 8, параграф 2, буква в).

145 *Пак там.*

146 *Пак там*, член 8, параграф 2, буква б).

147 *Пак там,* член 8, параграф 2, буква г).

- когато чувствителни данни се използват в контекста на съдебно производство пред съд или административен орган за предявяването, изпълнението или защитата на правен иск[148].

Освен това съгласно член 8, параграф 3 от Директивата за защита на личните данни, когато здравни данни се използват за медицински преглед и лечение от доставчици на здравни услуги, управлението на тези услуги се включва в обхвата на това изключение. Като специална гаранция лицата се признават за „доставчици на здравни грижи“ само ако са обвързани със специални професионални задължения за поверителност.

Обществен интерес

Освен това в съответствие с член 8, параграф 4 от Директивата за защита на личните данни държавите членки могат да въведат допълнителни цели, за които могат да се обработват чувствителни данни, при условие че:

- обработването на данни е по съображения, свързани със значим обществен интерес; и

- то е предвидено в националното законодателство или е вследствие на решение на надзорния орган; и

- в националното законодателство или с решение на надзорния орган се определят необходимите гаранции за ефективната защита на интересите на физическите лица[149].

Известен пример са системите за електронни здравни досиета, които са на път да бъдат въведени в много държави членки. Тези системи позволяват здравни данни, събирани от доставчиците на здравни услуги в хода на лечението на даден пациент, да се предоставят на други доставчици на здравни услуги на този пациент в голям мащаб, обикновено в национален мащаб.

Работната група по член 29 достигна до заключението, че такива системи не могат да бъдат създадени въз основа на съществуващите правни норми за обработване на данни относно пациенти, основаващи се на член 8, параграф 3

148 *Пак там*, член 8, параграф 2, буква д).

149 *Пак там*, член 8, параграф 4.

от Директивата за защита на личните данни. Ако обаче приемем, че съществуването на такива системи за електронни здравни досиета представлява значим обществен интерес, тогава то би могло да се основава на член 8, параграф 4 от директивата, в който се изисква изрично правно основание за тяхното създаване, което също така съдържа необходимите гаранции, за да се осигури сигурното функциониране на системата[150].

4.2. Правила относно сигурността на обработването

Ключови въпроси

- Правилата относно сигурността на обработването съдържат задължение за администратора и обработващия да прилагат подходящи технически и организационни мерки, за да се предотврати всякаква неразрешена намеса в операциите по обработване на данни.
- Необходимото ниво на сигурност на данните се определя от:
  - средствата за гаранитране на сигурността, достъпни на пазара за всеки отделен вид обработване; и
  - разходите; и
  - чувствителността на обработваните данни.
- Сигурното обработване на данни е защитено допълнително от общото задължение на всички лица, администратори или обработващи да гарантират, че данните остават поверителни.

Задължението на администраторите и обработващите да разполагат с въведени адекватни мерки, за да гарантират сигурността на данните, следователно е установено в **правото на Съвета на Европа в областта на защитата на данните**, както и **в това на ЕС**.

150 Работна група за защита на личните данни по член 29 (2007 г.), *Работен документ относно обработването на лични здравни данни в електронните здравни досиета (ЕЗД)*, WP 131, Брюксел, 15 февруари 2007 г.

4.2.1. Елементи на сигурността на данните

Съгласно съответните разпоредби на **правото на ЕС**:

> *„Държавите членки предвиждат, че администраторът трябва да прилага подходящи технически и организационни мерки за защита на личните данни срещу случайно или неправомерно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп, в частност, когато обработването включва предаване на данните по мрежа, както и срещу всякакви други незаконни форми на обработка"*[151].

Подобна разпоредба съществува съгласно **правото на Съвета на Европа**:

> *„Трябва да бъдат взети подходящи мерки за сигурност с цел защита на личните данни, запаметени в автоматизирани регистри, срещу случайно или непозволено унищожаване или случайна загуба, както и срещу непозволен достъп, изменение или разпространение"*[152].

Често има също така отраслови, национални и международни стандарти, които са били изготвени с цел сигурно обработване на данни. Европейският печат за неприкосновеност на личния живот (EuroPriSe) например е проект по програма eTEN (Трансевропейски телекомуникационни мрежи) на ЕС, в който са проучени възможностите за сертифициране на продукти, особено софтуер, като съответстващи на европейското право зазащита на данните. Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) беше създадена, за да увеличи възможностите на ЕС, на държавите членки на ЕС, и на деловата общност за предотвратяване, разглеждане и разрешаване на проблемите на мрежовата и информационната сигурност[153]. ENISA редовно публикува анализи на настоящите заплахи за сигурността и съвети относно начините за справяне с тях.

Сигурността на данните не се постига само с наличието на правилното оборудване — хардуер и софтуер. За това се изискват също така подходящи

151 Директива за защита на личните данни, член 17, параграф 1.

152 Конвенция 108, член 7.

153 Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. относно създаване на Европейската агенция за мрежова и информационна сигурност, ОВ L 77, 13.3.2004 г.

вътрешни организационни правила. Подобни вътрешни правила биха обхващали в идеалния случай следните въпроси:

- редовно предоставяне на всички служители на информация относно правилата за сигурност на данните и техните задължения съгласно правото зазащита на данните, особено по отношение на техните задължения за поверителност;

- ясно разпределяне на задълженията и ясно очертаване на правомощията по въпроси, свързани с обработването на данни, особено във връзка с взимане на решения за обработване на лични данни и за трансфер на данни към трети страни;

- използване на лични данни само в съответствие с инструкциите на компетентното лице или в съответствие с установените общи правила;

- защита на достъпа до местонахожденията и до хардуера и софтуера на администратора или на обработващия, включително проверки относно разрешението за достъп;

- гарантиране, че разрешенията за достъп до лични данни са били дадени от компетентното лице, и изискване на надлежна документация;

- автоматизирани протоколи относно достъпа до лични данни чрез електронни средства и редовни проверки на тези протоколи от вътрешната надзорна служба;

- точна документация за други форми на разкриване, различни от автоматизирания достъп до данни, за да има възможност да се докаже, че не е осъществено незаконно предаване на данни.

Важен елемент от ефективните предпазни мерки, свързани със сигурността, е и предлагането на подходящо обучение и образование по въпросите на сигурността на данните на членовете на персонала . Трябва да бъдат въведени и процедури за проверка, за да се гарантира, че съответните мерки съществуват не само на хартия, а се прилагат, и функционират на практика (като например вътрешни или външни одити).

Мерките, които се използват от администратора или обработващия за подобряване на степента на сигурност включват инструменти, като например длъжностни лица за защита на личните данни, образование на служителите по въпросите на сигурността, редовни одити, тестване на вероятни пробиви и печати за качество.

Пример: В решението по дело *I./Финландия*[154] жалбоподателката не е била в състояние да докаже, че други служители на болницата, в която е работела, са имали незаконен достъп до нейното здравно досие. Поради това нейният иск за нарушаване на правото ѝ на защита на данните е бил отхвърлен от националните съдилища. ЕСПЧ е заключил, че е налице нарушение на член 8 от ЕКПЧ, тъй като системата на болницата за вписване в здравните досиета „била такава, че не било възможно със задна дата да се изясни използването на данни за пациента, тъй като тя показвала само петте най-скорошни консултации, и че тази информация била заличавана веднага след връщането на досието в архива". Решаващо за съда било, че въведената в болницата система за вписване на данни явно не била в съответствие с правните изисквания, съдържащи се в националното законодателство — факт, на който националните съдилища не са отдали подобаващо значение.

Уведомления за нарушения на сигурността на данните

В законодателството за защита на данните на няколко европейски държави беше въведен нов инструмент за справяне с нарушенията на сигурността на данните: задължение на доставчиците на електронни съобщителни услуги да уведомяват вероятните потърпевши и надзорните органи за нарушения на сигурността на данните. За доставчиците на далекосъобщителни услуги това е задължително съгласно правото на ЕС[155]. Целта на уведомяването на

154 ЕСПЧ, Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03.

155 Вж. Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации, *(Директива за правото на неприкосновеност на личния живот и електронни комуникации),* ОВ L 201, 31.7.2002 г., член 4, параграф 3, изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите, ОВ L 337, 18.12.2009 г.

съответните физически лица за нарушения на сигурността на данните е да се избегнат щетите: уведомлението за нарушения на сигурността на данните и възможните последици от тях свеждат до минимум риска от отрицателно въздействие за съответните физически лица. В случаите на груба небрежност доставчиците могат също така да бъдат глобени.

Ще бъде необходимо да се създадат предварително вътрешни процедури за ефективно управление и докладване на нарушенията на сигурността на данните, тъй като срокът за изпълнение на задължение за докладване на съответните физически лица и/или на надзорните органи съгласно националното законодателство обикновено е твърде кратък.

4.2.2. Поверителност

Съгласно правото на ЕС сигурното обработване на данни е защитено допълнително от общото задължение на всички лица, администратори или обработващи да гарантират, че данните остават поверителни.

Пример: Служителка в застрахователно дружество получава телефонно обаждане на работното си място от някой, който казва, че е клиент, като изисква информация, отнасяща се до неговия застрахователен договор.

Задължението за опазване на поверителността на данните на клиента изисква от служителката да приложи най-малко минимални мерки за сигурност преди да разкрие лични данни. Това например би могло да стане като предложи да върне обаждането на телефонен номер, документиран в досието на клиента.

Член 16 от Директивата за защита на личните данни се отнася до поверителността само в рамките на отношенията между администратор и обработващ. Дали администраторите трябва да запазват поверителността на данните, в смисъл да не могат да ги разкриват на трети лица, е разгледано в членове 7 и 8 от директивата.

Задължението за поверителност не обхваща ситуации, в които данните стават известни на лице в неговото качество на частно физическо лице, а не на служител на администратор или обработващ данни. В този случай не се прилага член 16 от Директивата за защита на личните данни, тъй като в

действителност използването на личните данни от частни физически лица е напълно изключено от обхвата ѝ, където подобно използване попада в рамките на т. нар. изключение за домашни дейности[156]. Изключението за домашни дейности е използването на лични данни „от физическо лице в хода на предимно лични или домашни занимания“[157]. След решението на Съда на ЕС по делото *Bodil Lindqvist*[158] обаче това изключение трябва да се тълкува ограничително, особено във връзка с разкриването на данни. По-специално, изключението за домашни дейности не обхваща публикуването на лични данни за неограничен брой получатели в интернет (за повече подробности по делото вж. раздели 2.1.2, 2.2, 2.3.1 и 6.1).

Съгласно правото на Съвета на Европа задължението за поверителност е включено в понятието за сигурност на данните в член 7 от Конвенция № 108, в който се разглежда сигурността на данните.

За обработващите поверителността означава, че те могат да използват лични данни, които са им били поверени от администратора, само в съответствие с дадените от него инструкции. Поради съображения за поверителност от служителите на администратора или на обработващия се изисква да използват личните данни само в съответствие с инструкциите на своите компетентни висшестоящи.

Задължението за поверителност трябва да бъде включено във всички договори между администраторите и съответните обработващи. Освен това, администраторите и обработващите ще трябва да вземат конкретни мерки за въвеждане на правното задължение за поверителност по отношение на своите служители, което обикновено се осъществява чрез включването на клаузи за поверителност в трудовия договор на служителя.

Нарушаването на професионалните задължения за поверителност е наказуемо съгласно наказателното право в много държави членки на ЕС, и страни по Конвенция № 108.

156 Директива за защита на личните данни, член 3, параграф 2, второ тире.

157 *Пак там*.

158 Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Lindqvist*, C-101/01.

4.3. Правила за прозрачност при обработването

Ключови въпроси

- Преди да започне обработването на лични данни администраторът трябва най-малкото да информира съответните физически лица за самоличността си и за целта на обработването на данните, освен ако съответното физическо лице вече не притежава тази информация.
- Когато данните се събират от трети лица, задължението за предоставяне на информация не се прилага, ако:
  - обработването на данните е предвидено от закона; или
  - предоставянето на информация се окаже невъзможно или би било свързано с прекомерни усилия.
- Преди да започне обработването на лични данни администраторът трябва освен това:
  - да уведоми надзорния орган за предвидените операции по обработването на данни; или
  - обработването да бъде документирано вътрешно от независимо длъжностно лице за защита на личните данни, ако националното законодателство предвижда подобна процедура.

Принципът за добросъвестно обработване изисква прозрачност на обработването. **Правото на Съвета на Европа** предвижда за тази цел, че на всяко лице трябва да се дава възможност да установи съществуването на регистри на обработваните лични данни, техните основни цели, както и отговорния администратор[159]. Определянето на начините, по които следва да се осъществи това, е предоставено на националното законодателство. **Правото на ЕС** е по-конкретно, като гарантира прозрачност за съответните физически лица чрез задължението на администратора да ги информира, и за обществеността чрез изпращането на уведомление.

Съгласно и двете правни системи, изключения и ограничения по отношение на задълженията за прозрачност на администратора могат да съществуват в националното законодателство, ако подобно ограничение представлява

159 Конвенция № 108, член 8, буква а).

необходима мярка за гарантиране на определени обществени интереси или за защита на съответното физическо лице или на правата и свободите на други лица, доколкото това е необходимо в едно демократично общество[160]. Подобни изключения могат да бъдат необходими например в контекста на разследване на престъпление, но също така могат да бъдат оправдани при други обстоятелства.

4.3.1. Информация

Съгласно правото на Съвета на Европа, както и правото на ЕС администраторите, които осъществяват операции по обработване на данни, са длъжни да информират предварително съответните физически лица за предвиденото обработване[161]. Това задължение не зависи от наличието на искане от страна на съответното физическо лице, а трябва да се изпълнява проактивно от администратора, независимо от това дали лицетопроявява интерес към информацията или не.

Съдържание на информацията

Информацията трябва да включва целта на обработването, както и самоличността на администратора и данните за връзка с него[162]. Директивата за защита на личните данни изисква предоставянето на допълнителна информация, когато подобна информация „е необходима, като се отчитат конкретните обстоятелства, при които се обработват данните, за гарантиране на справедливата им обработка по отношение на съответното физическо лице". В членове 10 и 11 от директивата са посочени, наред с другото, категориите обработвани данни и получателите на такива данни, както и наличието на право на достъп и право на коригиране на данните. Ако данните се събират от съответните физически лица, информацията следва да изяснява дали отговорите на въпросите са задължителни или доброволни, както и евентуалните последици при липса на отговор[163].

В контекста на **правото на Съвета на Европа** предоставянето на подобна информация може да се счита за добра практика съгласно принципа за

160 *Пак там*, член 9, параграф 2; и Директива за защита на личните данни, член 13, параграф 1.

161 Конвенция № 108, член 8, буква а); и Директива за защита на личните данни, членове 10 и 11.

162 Конвенция № 108, член 8, буква а); и Директива за защита на личните данни, член 10, букви а) и б).

163 Директива за защита на личните данни, член 10, буква в).

добросъвестно обработване на данните и в този смисъл то е също така част от правото на Съвета на Европа.

Принципът за добросъвестно обработване на данните изисква информацията да бъде лесно разбираема от съответните физически лица. Трябва да се използва език, който е подходящ за съответните адресати. Нивото и видът на използвания език би трябвало да бъдат различни в зависимост от това дали групата, за която е предназначен, са например възрастни хора или деца, обществеността или университетски експерти.

Някои физически лица ще искат да бъдат информирани само накратко относно това как и защо се обработват техните данни, докато други ще искат подробно разяснение. Начините за балансиране на този аспект на добросъвестното информиране са разгледани в становище на Работната група по член 29, която подкрепя идеята за т. нар. „многостепенни" съобщения[164], позволяващи на съответното физическо лице да реши какво ниво на информираност предпочита.

Момент на предоставяне на информацията

В Директивата за защита на личните данни се съдържат леко различаващи се разпоредби относно момента, в който информацията трябва да бъде предоставена, в зависимост от това дали данните се събират от съответните физически лица (член 10) или от трето лице (член 11). Когато данните се събират от съответното физическо лице, информацията трябва да бъде предоставена най-късно в момента на събирането. Когато данните се събират от трети лица, информацията трябва да бъде предоставена най-късно в момента, когато администраторът ги записва или преди данните да бъдат разкрити за първи път на трето лице.

Изключения от задължението за информиране

Съгласно правото на ЕС съществува общо изключение от задължението за информиране на съответното физическо лице, когато то вече притежава тази информация[165]. Това се отнася до ситуациите, когато съответното физическо

164 Работна група за защита на личните данни по член 29 (2004 г.), *Opinion 10/2004 on More Harmonised Information Provisions [Становище 10/2004 относно по-хармонизирани разпоредби за информацията]*, WP 100, Брюксел, 25 ноември 2004 г.

165 Директива за защита на личните данни, член 10 и член 11, параграф 1.

лице съобразно с обстоятелствата на случая вече знае, че неговите данни ще бъдат обработвани с определена цел от определен администратор.

Член 11 от директивата, който се отнася до задължението за информиране на съответното физическо лице, когато данните не са били получени от него, гласи също така, че не е налице подобно задължение, по-специално, при обработването за статистически цели или за целите на историческо или научно изследване, когато:

- предоставянето на подобна информация се оказва невъзможно; или
- е свързано с прекомерно усилие; или
- ако записът или разкриването е постановено изрично от закона[166].

Само в член 11, параграф 2 от Директивата за защита на личните данни се посочва, че не е необходимо съответните физически лица да бъдат информирани относно операциите по обработване на данни, ако те са постановени от закона. Предвид общоправната презумпция за познаване на закона от правните субекти, би могъл да се приведе доводът, че ако данните са събирани от съответното физическо лице съгласно член 10 от директивата, то вече притежава информацията. Но предвид факта, че познаването на закона е само презумпция, принципът за добросъвестно обработване би изисквал съгласно член 10 съответното физическо лице да бъде информирано дори ако обработването е постановено от закона, по-специално, тъй като предоставянето на информация на съответното физическо лице не е особено трудно, ако данните се събират непосредствено от него.

Що се отнася до правото на Съвета на Европа, Конвенция № 108 изрично предвижда изключения от своя член 8. Изключенията, посочени в членове 10 и 11 от Директивата за защита на личните данни, отново могат да се разглеждат като примери за добри практики по отношение на изключенията съгласно член 9 от Конвенция № 108.

Различни начини за предоставяне на информация

Най-добрият начин за предоставяне на информация би бил обръщение в устна или писмена форма към всяко отделно физическо лице. Ако данните

166 *Пак там*, съображение 40 и член 11 , параграф 2.

се събират от съответното физическо лице, предоставянето на информация следва да стане едновременно със събирането. Все пак, особено когато данните се събират от трети лица, предвид очевидните практически трудности да се достигне лично до съответните физически лица, информацията може да се предоставя и чрез подходяща публикация.

Един от най-ефективните начини за предоставяне на информация е наличието на подходящи клаузи относно информацията, качени на началната страница на администратора, като например политика за поверителност на уебсайта. Има обаче значителна част от населението, която не използва интернет, и информационната политика на дружеството или публичния орган трябва да предвиди това.

4.3.2. Уведомяване

Националното законодателство може да задължи администраторите да уведомят компетентния надзорен орган относно своите операции по обработване, така че те да могат да бъдат публикувани. Националното законодателство може да заложи, като алтернатива, администраторите да могат да назначават длъжностно лице за защита на личните данни, което основно даотговаря за водене на регистър на извършваните от администратора операции по обработване[167]. При поискване този вътрешен регистър трябва да бъде предоставен на членове на обществеността.

Пример: В уведомлението, както и в документацията, водена от вътрешното длъжностно лице за защита на личните данни, трябва да бъдат описани основните характеристики на въпросното обработване на данни. Това включва информация за администратора, целта и правното основание на обработването, категориите обработвани данни, вероятните получатели — трети лица, и дали са предвидени трансгранични потоци от данни или не и ако да, какви.

Публикуването на уведомленията от надзорния орган трябва да бъде под формата на специален регистър. За да постигне своята цел, достъпът до този регистър трябва да бъде лесен и безплатен. Същото се отнася за документацията, водена от длъжностното лице за защита на личните данни, назначено от администратора.

167 *Пак там*, член 18, параграф 2, второ тире.

В националното законодателство могат да бъдат предвидени изключения от задълженията за уведомяване на компетентния надзорен орган или за назначаване на вътрешно длъжностно лице за защита на данните, по отношение на операции по обработване, които няма вероятност да представляват конкретен риск за съответните физически лица, които са посочени в член 18, параграф 2 от Директивата за защита на личните данни[168].

4.4. Правила относно насърчаване на спазването на разпоредбите

Ключови въпроси

- Когато се развива принципът за отчетност, в Директивата за защита на личните данни се посочват няколко инструмента за насърчаване на спазването на разпоредбите:
  - предварителна проверка от страна на националния надзорен орган на планираните операции по обработване на данни;
  - длъжностни лица за защита на личните данни, които предоставят на администратора експертен опит в областта на защитата на данните;
  - кодекси за поведение, в които се определят съществуващите правила за защита на данните, за прилагане в дадена обществена сфера, особено в сферата на стопанска дейност.
- Правото на Съвета на Европа предлага подобни инструменти за насърчаване на спазването на разпоредбите в своята Препоръка относно профилирането.

4.4.1. Предварителна проверка

Съгласно член 20 от Директивата за защита на личните данни, надзорният орган трябва да провери операциите по обработване, които могат да създадат конкретен риск за правата и свободите на съответните физически лица поради целта или обстоятелствата на обработването, преди да бъдат започнати. Националното законодателство трябва да определи кои операции по обработване отговарят на условията за предварителна проверка. Подобна проверка може да доведе до забрана на операциите по обработване или

168 *Пак там*, член 18 , параграф 2, първо тире.

до разпореждане за промяна на предложения начин на извършване на тези операции. Член 20 от директивата има за цел да гарантира, че прекомерно рисковото обработване няма да бъде започвано, тъй като надзорният орган е оправомощен да забрани подобни операции. Необходимо условие за ефективността на този механизъм е надзорният орган да бъде действително уведомен. За да се гарантира, че администраторите изпълняват своето задължение за уведомяване, надзорните органи трябва да имат принудителни правомощия, като например възможността да глобяват администраторите.

Пример: Ако дружество осъществява операции по обработване на данни, които в съответствие с националното законодателство подлежат на предварителна проверка, то трябва да представи на надзорния орган документация за планираните такива операции. На дружеството не се разрешава да започне операциите по обработване преди да получи положителен отговор от надзорния орган.

В някои държави членки националното законодателство предвижда като алтернатива операциите по обработване да могат да бъдат започнати, ако няма реакция от надзорния орган в определен срок, като например в срок от три месеца.

4.4.2. Длъжностни лица за защита на личните данни

Директивата за защита на личните данни допуска възможността националното законодателство да предвиди, че администраторите могат да назначат служител, който да изпълнява функцията на длъжностно лице за защита на личните данни[169]. Целта на назначаването на подобно длъжностно лице е да се гарантира, че няма вероятност правата и свободите на физическите лица да бъдат неблагоприятно засегнати от операциите по обработване[170].

Пример: В Германия в съответствие с раздел 4е, подраздел 1 от германския Федерален закон за защита на личните данни (*Bundesdatenschutzgesetz*) от частните дружества се изисква да назначат вътрешно длъжностно лице

169 *Пак там*, член 18, параграф 2, второ тире.

170 *Пак там*.

за защита на личните данни, ако имат постоянно назначени 10 или повече лица в областта на автоматизираното обработване на лични данни.

Възможността за постигане на тази цел изисква определена степен на независимост на длъжностното лице в рамките на организацията на администратора, както е посочено изрично в директивата. Необходими са също така стабилни трудови права с цел защита срещу възможни сценарии, например неоснователно уволнение, за да се подкрепи ефективното функциониране на тази длъжност.

За да се насърчава спазването на националното законодателство за защита на данните, идеята за вътрешни длъжностни лица за защита на личните данни беше възприета и в някои от препоръките на Съвета на Европа[171].

4.4.3. Кодекси за поведение

С цел да се насърчи спазването на разпоредбите, стопанският и други сектори могат да разработват подробни правила, които да уреждат техните типични дейности по обработване, като кодифицират най-добрите практики. Експертният опит на членовете от сектора ще благоприятства намирането на решения, които са практически осъществими и следователно биха могли да бъдат прилагани. Съответно държавите членки и Европейската комисия се насърчават да подкрепят разработването на кодекси за поведение, които имат за цел да допринесат за правилното прилагане на националните разпоредби, приети от държавите членки в съответствие с директивата, като се отчитат специфичните характеристики на отделните сектори[172].

За да се гарантира, че тези кодекси за поведение са в синхрон с националните разпоредби, приети от държавите членки в съответствие с Директивата за защита на личните данни, страните членки трябва да въведат процедура за оценка на кодексите. Тази процедура обикновено би изисквала участието на националния орган, търговските сдружения и другите органи, представляващи други категории администратори[173].

171 Вж. например Препоръка относно профилирането, член 8.3.

172 Вж. Директивата за защита на личните данни, член 27, параграф 1.

173 *Пак там*, член 27, параграф 2.

Проектокодексите на Общността, както и измененията и допълненията към съществуващите кодекси на Общността, могат да се предават за оценка на Работната група по член 29. След одобрение от тази работна група, Европейската комисия може да осигури подходяща публичност на подобни кодекси[174].

Пример: Европейската федерация за директен маркетинг (FEDMA) разработи Европейски кодекс за практика при използването на лични данни при директен маркетинг. Кодексът беше представен успешно на Работната група по член 29. През 2010 г. към кодекса беше добавено приложение, отнасящо се до електронните маркетингови съобщения[175].

174 *Пак там*, член 27, параграф 3.

175 Работна група за защита на личните данни по член 29 (2010 г.), *Становище 4/2010 относно Европейския кодекс за поведение на Европейската федерация за директен маркетинг (FEDMA) за използването на лични данни при директен маркетинг*, WP 174, Брюксел, 13 юли 2010 г.

5

Правата на съответното физическо лице и тяхното прилагане

ЕС	Обхванати въпроси	Съвет на Европа
Право на достъп		
Директива за защита на личните данни, член 12 Съд на ЕС, Решение от 7 май 2009 г. по дело *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07	**Право на достъп на дадено лице до собствените му данни**	Конвенция № 108, член 8, буква б)
	Право на коригиране, на изтриване (заличаване) или на блокиране	Конвенция № 108, член 8, буква в) ЕСПЧ, Решение от 18 ноември 2008 г. по дело *Cemalettin Canli/Турция*, № 22427/04 ЕСПЧ, Решение от 6 юни 2006 г. по дело *Segerstedt-Wibergu други/Швеция*, № 62332/00 ЕСПЧ, Решение от 27 април 2010 г. по дело *Ciubotaru/Молдова*, № 27138/04
Право на възражение		
Директива за защита на личните данни, член 14, параграф 1, буква а)	**Право на възражение, свързано с конкретното положение на физическото лице**	Препоръка относно профилирането, член 5.3

Директива за защита на личните данни, член 14, параграф 1, буква б)	**Право на възражение срещу бъдещо използване на данните за маркетингови цели**	Препоръка относно директния маркетинг, член 4.1
Директива за защита на личните данни, член 15	**Право на възражение срещу автоматизирани решения**	Препоръка относно профилирането, член 5.5
Независим надзор		
Харта, член 8, параграф 3 Директива за защита на личните данни, член 28 Регламент относно защитата на данните при обработването им от институции на ЕС, глава V Регламент относно защитата на данните Съд на ЕС, Решение от 9 март 2010 г. по дело *Европейска комисия/Федерална република Германия*, C-518/07 Съд на ЕС, Решение от 16 октомври 2012 г. по дело *Европейска комисия/Република Австрия*, C-614/10 Съд на ЕС, *8 април 2014 г.* по дело *Европейска комисия/Унгария*, C-288/12	**Национални надзорни органи**	Конвенция № 108, Допълнителен протокол, член 1
Средства за правна защита и санкции		
Директива за защита на личните данни, член 12	**Искане, отправено към администратора**	Конвенция № 108, член 8, буква б)
Директива за защита на личните данни, член 28, параграф 4 Регламент относно защитата на данните при обработването им от институции на ЕС, член 32, параграф 2	**Жалби, подадени до надзорен орган**	Конвенция № 108, Допълнителен протокол, член 1, параграф 2, буква б)
Хартата, член 47	**Съдилища (общо по въпроса)**	ЕКПЧ, член 13
Директива за защита на личните данни, член 28, параграф 3	**Национални съдилища**	Конвенция № 108, Допълнителен протокол, член 1, параграф 4

ДФЕС, член 263, параграф 4 Регламент относно защитата на данните при обработването им от институции на ЕС, член 32, параграф 1 ДФЕС, член 267	**Съд на ЕС**	
	ЕСПЧ	ЕКПЧ, член 34
Средства за правна защита и санкции		
Хартата, член 47 Директива за защита на личните данни, членове 22 и 23 Съд на ЕС, Решение от 10 април 1984 г. по дело *Sabine von Colson u Elisabeth Kamann/Land Nordrhein-Westfalen*, C-14/83 Съд на ЕС, Решение от 26 февруари 1986 г. по дело *M. H. Marshall/Southampton u South-West Hampshire Area Health Authority*, C-152/84	**За нарушения на националното законодателство за защита на данните**	ЕКПЧ, член 13 (само за държави членки на Съвета на Европа) Конвенция № 108, член 10 ЕСПЧ, Решение от 2 март 2008 г. по дело *K.U./Финландия*, № 2872/02 ЕСПЧ, Решение от 25 ноември 2008 г. по дело *Biriuk/Литва*, № 23373/03.
Регламент относно защитата на данните при обработването им от институции на ЕС, членове 34 и 49 Съд на ЕС, Решение от 29 юни 2010 г. по дело *Европейска комисия/The Bavarian Lager Co. Ltd*, C-28/08 P	**За нарушения на правото на ЕС от страна на институции или органи на ЕС**	

Ефективността на правните норми като цяло и по-конкретно, на правата на физическите лица, зависи до голяма степен от наличието на подходящи механизми за прилагането им. В европейското право за защита на данните физическото лице трябва да бъде оправомощено от националното законодателство да защитава своите данни. Освен това съгласно националното законодателство трябва да бъдат създадени независими надзорни органи, които да подпомагат физическите лица при упражняването на техните права, както и да осъществяват контрол върху обработването на лични данни. В допълнение, правото на ефективни средства за правна защита, гарантирано от ЕКПЧ и Хартата, налага всяко лице да разполага със средства за правна защита.

5.1. Правата на физическите лица

Ключови въпроси

- Всеки има право, съгласно националното законодателство, да изиска от който и да било администратор информация за това дали администраторът обработва негови данни.
- Съгласно националното законодателство физическите лица имат правото:
  - да получат достъп до собствените си данни от всеки администратор, който обработва тези данни;
  - данните им да бъдат коригирани (или блокирани, според случая) от администратора, който обработва данните им, ако тези данни са неточни;
  - данните им да бъдат изтрити или блокирани, според случая, от администратора, ако последният обработва тези данни незаконно.
- В допълнение физическите лица имат правото да предявяват възражения пред администраторите срещу:
  - автоматизирани решения (които се взимат чрез използване на лични данни, обработвани единствено с автоматизирани средства);
  - обработването на техните данни, ако това води до непропорционални резултати;
  - използването на техните данни за целите на директен маркетинг.

5.1.1. Право на достъп

Съгласно правото на ЕС – член 12 от Директивата за защита на личните данни съдържа елементи, свързани с правото на даденото физическо лице на достъп, включително правото да получи от администратора „потвърждение за това, дали отнасящи се до него данни се обработват, както и информация, най-малкото, за целите на тази обработка, категориите данни и получателите или категориите получатели, на които данните се разкриват“, както и да изиска коригиране, изтриване или блокиране „на данните, чиято обработка не е в съответствие с разпоредбите на настоящата директива, и по-конкретно поради непълнота или неточност на самите данни“.

В правото на Съвета на Европа съществуват същите тези права и те трябва да бъдат предвидени в националното законодателство (член 8 от Конвенция № 108). В няколко препоръки на Съвета на Европа се използва терминът „достъп", а различните аспекти на правото на достъп са описани и предложени за прилагане в националното законодателство по същия начин, по който това е посочено в горния параграф.

Съгласно член 9 от Конвенция № 108 и член 13 от Директивата за защита на личните данни задължението на администраторите да отговорят на искане за достъп на физическото лице може да бъде ограничено в резултат на преимуществени законни интереси на други лица. Преимуществените законни интереси могат да включват обществени интереси като национална сигурност, обществена сигурност и наказателно преследване на престъпления, както и частни интереси, които са по-основателни от интересите, свързани със защитата на данните.Всички изключения или ограничения трябва да бъдат необходими в едно демократично общество и те трябва да са пропорционални на преследваната цел. В много извънредни случаи, например поради медицински показания, защитата на физическото лице сама по себе си може да налага ограничение по отношение на прозрачността; това е свързано по-специално с ограничаване на правото на достъп на всяко физическо лице.

Всеки път, когато данните се обработват единствено за целите на научни изследвания или за статистически цели, Директивата за защита на личните данни позволява правата на достъп да бъдат ограничени от националното законодателство; въпреки това налице трябва да бъдат и подходящи правни гаранции. По-специално трябва да се гарантира, че във връзка с това обработване на данни не се вземат никакви мерки или решения относно конкретно лице и че „очевидно не съществува никакъв риск от накърняване на личния живот на съответното физическо лице"[176]. Подобни разпоредби се съдържат в член 9, параграф 3 от Конвенция № 108.

Правото на достъп на дадено лице до собствените му данни

Съгласно правото на Съвета на Европа правото на достъп до собствените данни на дадено лице е изрично признато в член 8 от Конвенция № 108. ЕСПЧ многократно е постановявал, че дадено лице има право на достъп до информация за неговите лични данни, съхранявани или използвани от други лица,

176 Директива за защита на личните данни, член 13, параграф 2.

както и че това право произтича от необходимостта да се зачита личният живот[177]. В решението по делото *Leander*[178] ЕСПЧ заключи, че правото на достъп до лични данни, съхранявани от публичните органи, може обаче да бъде ограничено при определени обстоятелства.

Съгласно правото на ЕС правото на достъп до собствените данни е изрично признато в член 12 от Директивата за защита на личните данни и — като основно право — в член 8, параграф 2 от Хартата.

В член 12, параграф а) от директивата се предвижда, че държавите членки трябва да гарантират, че всяко физическо лице има право на достъп до неговите лични данни и на информация. По-специално, всяко физическо лице има право да получи от администратора „потвърждение за това, дали отнасящи се до него данни се обработват, както и информация най-малкото за следното:

- целите на обработването;
- съответните категории данни;
- данните, които се обработват;
- получателите или категориите получатели, на които се разкриват данните;
- всякаква налична информация за източника на данните, които са в процес на обработване;
- в случи на автоматизирани решения — логиката на всяко автоматизирано обработване на данни.

В националното законодателство може да се добави допълнителна информация, която да се дава от администратора, например посочването на правното основание, въз основа на което е разрешено обработването на данни.

177 ЕСПЧ, Решение от 7 юли 1989 г. по дело *Gaskin/Обединеното кралство*, № 10454/83; ЕСПЧ, Решение от 13 февруари 2003 г. по дело *Odièvre/Франция* [голям състав], № 42326/98; ЕСПЧ, Решение от 28 април 2009 г. по дело *K.H и други/Словакия*, № 32881/04; ЕСПЧ, Решение от 25 септември 2012 г. по дело *Godelli/Италия*, № 33783/09.

178 ЕСПЧ, Решение от 11 юли 1985 г. по дело *Leander/Швеция*, № 9248/81.

Пример: Едно лице може да определи чрез получаване на достъп до личните данни на някого дали тези данни са точни. По тази причина, уведомяването на физическото лице за категориите обработвани данни, както и за съдържанието на данните, е неразделна част от процедурата. От това следва, че не е достатъчно администраторът просто да съобщи на физическото лице, че той обработва неговото име, адрес, дата на раждане и област на интереси. Администраторът трябва да съобщи на физическото лице, и че той обработва „името: N.N.; адрес: 1040 Vienna, Schwarzenbergplatz 11, Austria; датата на раждане: 10.10.1974 г. и областта на интереси (съгласно декларацията на физическото лице): класическа музика." Последният елемент съдържа в допълнение и информация за източника на данни.

Съобщението до физическото лице относно данните, които са в процес на обработване, и цялата налична информация относно източника им, трябва да бъде в разбираема форма, което означава, че може да е необходимо администраторът да обясни на физическото лице по-подробно какво точно обработва той. Например само цитирането на технически съкращения или медицински термини в отговор на искане за достъп обикновено не е достатъчно дори, когато се съхраняват само такива съкращения или термини.

В отговор на искане за достъп, администраторът трябва да предоставя информация за източника на данни, обработвани от него до степента, в която той разполага с такава информация. Тази разпоредба трябва да се разбира в светлината на принципите на добросъвестност и отчетност. Администраторът не може да унищожава информация за източника на данни, за да бъде освободен от задължението за разкриването му, нито пък може да пренебрегне обичайния стандарт и потвърдените потребности от документиране на извършваните от него дейности. Обикновено неводенето на документация относно източника на данните, които се обработват, представлява неизпълнение на задълженията на администратора съгласно правото на достъп.

Когато се извършват автоматизирани оценки, е необходимо да бъде разяснена общата логика на оценката, включително конкретните критерии, които са били взети предвид при оценяването на физическото лице.

Директивата не изяснява дали правото на достъп до информация се отнася за минал момент и ако това е така, за какъв минал период. В тази връзка, както е посочено в съдебната практика на Съда на ЕС, правото на достъп до

данните на дадено лице не може да бъде ограничавано неправомерно от времеви рамки. Освен това на физическите лица трябва да бъде предоставяна разумна възможност за получаване на информация относно операции по обработване на данни за минали периоди.

Пример: В делото *Rijkeboer*[179] от Съда на ЕС беше поискано да определи дали съгласно член 12, буква а) от директивата правото на дадено лице на достъп до информация относно получателите или категориите получатели на личните данни и относно съдържанието на данните може да бъде ограничено до една година, предхождаща искането му за достъп.

За да определи дали в член 12, буква а) от директивата се разрешава такова времево ограничение, Съдът реши да тълкува този член с оглед на целите на директивата. Съдът първо посочи, че правото на достъп е необходимо, за да позволи на съответното физическо лице да упражни правото да изиска отадминистратора да поправи, изтрие или блокира неговите данни (член 12, буква б)) или да го накара да уведоми третите лица, на които са разкрити данните, за поправките, изтриването или блокирането (член 12, буква в)). Правото на достъп е необходимо и за да се позволи на съответното физическо лице да упражни правото си на възражение срещу обработването на неговите лични данни (член 14) или правото си на иск в случай на претърпени вреди (членове 22 и 23).

За да се гарантира полезният ефект на горепосочените разпоредби, Съдът постанови, че „това право трябва задължително да се отнася за минал момент. Всъщност, ако случаят не е такъв, заинтересованото лице не би могло ефикасно да упражни правото си да иска поправка, изтриване или блокиране на данните, за които предполага, че са непълни или неточни, както и да предяви съдебен иск и да получи обезщетение за претърпените вреди“.

Правото на коригиране, изтриване и блокиране на данните

„Всяко лице трябва да може да упражнява правото си на достъп до данните, свързани с него, които се обработват, за да провери, в частност, точността на

179 Съд на ЕС, Решение от 7 май 2009 г. по дело *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, C-553/07.

данните и законосъобразността на обработването“[180]. В съответствие с тези принципи физическите лица трябва да имат правото, съгласно националното законодателство, да изискат от администратора коригиране, изтриване или блокиране на своите данни, ако считат, че тяхното обработване не е в съответствие с директивата, по-специално, поради неточния или непълния характер на данните[181].

Пример: В делото *Cemalettin Canli/Турция*[182] Европейският съд по правата на човека констатира нарушение на член 8 от ЕКПЧ, свързано с неточно изготвени полицейски доклади в рамките на наказателно производство.

Жалбоподателят е бил обект два пъти на наказателно производство заради предполагаемо участие в незаконни организации, но не е бил осъждан. При нов арест на жалбоподателя по обвинение в друго престъпление полицията е внесла в наказателния съд доклад, озаглавен *„информационен формуляр за допълнителни престъпления“*, в който жалбоподателят е представен като член на две незаконни организации. Искането на жалбоподателя да получи доклада и полицейското досие не е удовлетворено. ЕСПЧ приема, че информацията в полицейския доклад попада в обхвата на член 8 от ЕКПЧ, тъй като публичната информация също би могла да попадне в обхвата на понятието „личен живот“, когато тя е обект на системно събиране и съхранение от страна на органите. В допълнение на това полицейският доклад е бил неточен и неговото изготвяне и внасяне в наказателния съд не е било извършено в съответствие със закона. Съдът е заключил, че е налице нарушение на член 8.

Пример: В делото *Segerstedt-Wiberg и други/Швеция*[183] жалбоподателите са били обвързани с някои либерални и комунистически политически партии. Те подозират, че свързана с тях информация е била включена в тайни полицейски доклади. ЕСПЧ е счел, че съхраняването на спорните данни е правно обосновано и преследва основателна цел. По отношение на някои от жалбоподателите ЕСПЧ е констатирал, че продължащото съх-

180 Директива за защита на личните данни, съображение 41.

181 *Пак там*, член 12, буква б).

182 ЕСПЧ, Решение от 18 ноември 2008 г. по дело *Cemalettin Canli/Турция*, № 22427/04, точки 33, 42 и 43; ЕСПЧ, Решение от 2 февруари 2010 г. по дело *Dalea/Франция*, № 964/07.

183 ЕСПЧ, Решение от 6 юни 2006 г. по дело *Segerstedt-Wibergи други/Швеция*, № 62332/00, точки 89 и 90; вж. също например Решение от 18 април 2013 г. по дело *М.К./Франция*, № 19522/09.

ранение на данните представлява непропорционална намеса в личния живот. Например в случая с г-н Schmid органите са запазили информация, че през 1969 г. за него се е твърдяло, че е оказал насилствена съпротива при проверка от страна на полицията по време на демонстрации. ЕСПЧ е счел, че тази информация не би могла да представлява интерес с оглед на националната сигурност, особено предвид нейната давност. ЕСПЧ е заключил, че този случай представлява нарушение на член 8 от ЕКПЧ по отношение на четирима от петимата жалбоподатели.

В някои случаи е достатъчно физическото лице просто да поиска коригиране, например на начина на изписване на името, промяна на адрес или на телефонен номер. Ако обаче подобни искания са свързани с въпроси от правен характер, като например правната самоличност на физическото лице или точното местожителство с оглед връчването на правни документи, исканията за коригиране може да се окажат недостатъчни и администраторът може да има право да поиска твърдението за неточност на данните да бъде доказано. Подобни искания не трябва да налагат непосилна тежест на доказване на физическите лица и по този начин да ги възпират да искат коригиране на свързаните с тях данни. ЕСПЧ установи нарушение на член 8 от ЕКПЧ в няколко случая, при които жалбоподателят не е имал възможност да оспори точността на информация, пазена в секретни архиви[184].

Пример: В делото *Ciubotaru/Молдова*[185] жалбоподателят не е могъл да промени своя, регистриран в официалните регистри, етнически произход от молдовски на румънски с аргумента, че не е успял да обоснове искането си. ЕСПЧ е счел, че е приемливо държавите да изискват обективни доказателства при регистрацията на етническата идентичност на отделните лица. Ако такова искане се основава на чисто субективни и необосновани причини, органите биха могли да го отхвърлят. Въпреки това, претенцията на жалбоподателя е била основана на нещо повече от субективното възприятие за собствената му етническа принадлежност, като той е бил в състояние да предостави обективно проверими връзки с румънската етническа група като език, име, светоусещане и т.н. Въпреки това, съгласно националното законодателство, жалбоподателят е бил задължен да предостави доказателство за принадлежността на родителите си към румънската етническа група. Предвид историческата

184 ЕСПЧ, Решение от 4 май 2000 г. по дело *Rotaru/Румъния*, № 28341/95.

185 ЕСПЧ, Решение от 27 април 2010 г. по дело *Ciubotaru/Молдова*, № 27138/04, точки 51 и 59.

реалност в Молдова подобно искане е създало непреодолима пречка пред регистрацията на етническа идентичност, различна от онази, която съветските власти са посочили по отношение на родителите му. Възпрепятствайки разглеждането на искането на жалбоподателя в светлината на обективно проверими доказателства, държавата не е изпълнила своето позитивно задължение да осигури на жалбоподателя ефективно зачитане на неприкосновеността на личния му живот. Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

В хода на граждански спорове или производства пред публичен орган, когато се решава дали дадени данни са точни или не, физическото лице може да изиска в досието с неговите данни да бъде добавен коментар или бележка, които да посочват, че точността им се оспорва и че предстои вземането на официално решение. Докато това се случи, администраторът не трябва да представя данните за сигурни или окончателни, особено пред трети лица.

Искането на физическо лице за изтриване или заличаване на данни често се основава на твърдението, че обработването на данните не е правно обосновано. Подобни твърдения често възникват при оттегляне на съгласие или в случаите, когато дадени данни вече не са необходими за изпълнението на целите, за които са били събрани. Тежестта, свързана с доказването на законосъобразността на обработването на данните, се носи от администратора, тъй като той отговаря за законосъобразността на обработването. Съгласно принципа за отчетност администраторът трябва във всеки момент да може да докаже, че е налице стабилна правно основание за обработването на данните, като в противен случай обработването трябва да бъде прекратено.

В случай че обработването на данните бъде оспорено заради твърдение за неправилно или незаконосъобразно обработване, физическото лице, в съответствие с принципа за добросъвестно обработване, може да поиска данните, предмет на спора, да бъдат блокирани. Това означава, че данните не се заличават, но администраторът трябва да се въздържа да ги използва за срока на блокирането. Това е особено необходимо в случаите, когато продължаващото използване на неточни или незаконно притежавани данни би могло да причини вреда на физическото лице. Националното законодателство следва да предоставя по-подробна информация относно това кога възниква задължението за блокиране на използването на данните и как следва да се упражнява то.

Физическите лица освен това имат право да изискат от администратора да изпрати уведомление до трети лица относно блокиране, коригиране или изтриване, ако те са получили данните преди операциите по обработване. Тъй като разкриването на данни пред трети лица трябва да е било документирано от администратора, следва да е възможно идентифицирането на получателите на данните и искането на заличаване. Въпреки това, ако междувременно данните са били публикувани, например в интернет, може да е невъзможно данните да бъдат заличени във всички случаи, тъй като техните получатели не могат да бъдат намерени, „освен ако това се окаже невъзможно или е свързано с прекомерни усилия". Съгласно Директивата за защита на личните данни осъществяването на контакт с получателите на данните за коригирането, изтриването или блокирането на данните е задължително „освен ако това се окаже невъзможно или е свързано с прекомерни усилия"[186].

5.1.2. Право на възражение

Правото на възражение включва правото на възражение срещу индивидуални автоматизирани решения, правото на възражение, свързано с конкретното положение на физическото лице, и правото на възражение срещу бъдещо използване на данните за целите на директен маркетинг.

Право на възражение срещу индивидуални автоматизирани решения

Автоматизирани решения са решения, взети въз основа на лични данни, обработени само с автоматизирани средства. Ако съществува вероятност такива решения да имат съществено въздействие върху живота на лицата, които те касаят, например тяхната кредитоспособност, резултатите от работата им, поведението или надеждността им, е необходима специална защита с цел избягване на неподходящи последици. Директивата за защита на личните данни предвижда, че автоматизираните решения не трябва да засягат въпроси, които са важни за лицата, и изисква те да имат правото да прегледат въпросното автоматизирано решение[187].

Пример: Важен пример за автоматизирано решение от практиката е изготвянето на оценката при кандидатстване за кредит. С цел да се вземе

186 Директива за защита на личните данни, член 12, буква в), последна част от изречението.

187 *Пак там*, член 15, параграф 1.

бързо решение относно кредитоспособността на бъдещ клиент от него се събират някои данни, като например професионално или семейно положение, и се комбинират с данните за лицето от други източници, като например системите за кредитна информация. Тези данни автоматично се вкарват в алгоритъм за оценка, който изчислява общата стойност, отговаряща на кредитоспособността на потенциалния клиент. По този начин служителят на дружеството може да реши в рамките на няколко секунди дали физическото лице може да бъде одобрено за клиент или не.

Въпреки това съгласно директивата държавите членки постановяват, че дадено лице може да бъде предмет на индивидуално автоматизирано решение, при условие че интересите на физическото лице или не са застрашени, тъй като решението е в полза на физическото лице, или че те са гарантирани по друг подходящ начин[188]. Право на възражение срещу автоматизирани решения се предвижда и в **правото на Съвета на Европа**, както може да се види в Препоръката относно профилирането[189].

Право на възражение, свързано с конкретното положение на физическото лице

Не съществува общо право, по силата на което физическите лица могат да възразят срещу обработването на техните данни[190]. Въпреки това член 14, буква а) от Директивата за защита на личните данни дава право на съответното физическо лице да възразивъз основа на неопровержими законни основания, свързани с неговото конкретно положение. Подобно право е признато и в Препоръката относно профилирането на Съвета на Европа[191]. Тези разпоредби целят да се намери правилния баланс между правата на физическото лице, свързани със защитата на личните му данни, и законните права на други лица да обработват данните на съответното физическо лице.

Пример: Банка съхранява за срок от седем години данни за клиентите си, които са неизрядни в плащанията. Клиент, чиито данни се съхраняват

188 *Пак там*, член 15, параграф 2.

189 Препоръка относно профилирането, член 5, параграф 5.

190 Вж. също ЕСПЧ, Решение от 27 август 1997 г. по дело *M.S./Швеция*, № 20837/92, в което медицински данни са били съобщени без предоставянето на съгласие или възможност за възражение; или ЕСПЧ, Решение от 26 март 1987 г. по дело *Leander/Швеция*, № 9248/81; или ЕСПЧ, Решение от 10 май 2011 г. по дело *Mosley/Обединеното кралство*, № 48009/08.

191 Препоръка относно профилирането, член 5, параграф 3.

във въпросната база данни, кандидатства за нов заем. Прави се справка в базата данни, извършва се оценка на финансовото положение и клиентът получава отказ на молбата си за заем. Клиентът обаче може да възрази срещу записването на личните му данни в базата данни и да изиска заличаването на данните, ако той може да докаже, че неизрядното плащане е просто резултат на грешка, която е била поправена незабавно, след като клиентът е узнал за нея.

Резултатът от успешно възражение се състои в това, че администраторът не може повече да обработва въпросните данни. Операциите по обработването на данните на физическото лице, извършени преди възражението, обаче продължават да бъдат законни.

Правото на възражение срещу бъдещо използване на данните за целите на директен маркетинг

Член 14, буква б) от Директивата за защита на личните данни предвижда специално право на възражение срещу използването на личните данни на дадено лице за целите на директен маркетинг. Подобно право се предвижда също и в Препоръката на Съвета на Европа относно директния маркетинг[192]. Такъв тип възражения следва да се подават преди данните да бъдат предоставени на трети лица за целите на директен маркетинг. Следователно физическото лице трябва да има възможност да възрази преди трансфера на данните.

5.2. Независим надзор

Ключови въпроси

- С цел да се гарантира ефективна защита на данните националното законодателство трябва да предвижда създаването на независими надзорни органи.
- Националните надзорни органи трябва да действат напълно независимо, което трябва да бъде гарантирано от учредителния акт и да намира отражение в специфичната организационна структура на надзорния орган.

192 Съвет на Европа, Комитет на министрите (1985 г.), Препоръка Rec(85)20 до държавите членки относно защитата на лични данни, използвани за целите на директен маркетинг, 25 октомври 1985 г., член 4, параграф 1.

- Надзорните органи имат конкретна задача, наред с другото:
  - да наблюдават и насърчават защитата на данните на национално равнище;
  - да съветват физическите лица и администраторите, както и правителството и обществеността като цяло;
  - да изслушват жалбите и да помагат на физическите лица при твърдения за нарушения на правата, свързани със защитата на данните;
  - да упражняват надзор над администраторите и обработващите;
  - да се намесват при необходимост, като:
    - отправят предупреждение, строга забележка и дори глобяват администраторите и обработващите,
    - разпореждат коригиране, блокиране или изтриване на данни,
    - налагат забрана за обработване;
  - да сезират съда по конкретни случаи.

Директивата за защита на личните данни изисква въвеждането на независим надзор като важен механизъм за гарантиране на ефективна защита на личните данни. Директивата въвежда инструмент за прилагане на защитата на данните, който първоначално не е включен в Конвенция № 108 или в Насоките на ОИСР за защита на неприкосновеността на личния живот.

Предвид факта, че независимият надзор се оказа необходим за разработването на ефективна защита на личните данни, в нова разпоредба от ревизираните насоки на ОИСР от 2013 г., държавите членки се призовават „да установят и поддържат правоприлагащи органи в областта на защитата на неприкосновеността на личния живот, които да разполагат с управлението, ресурсите и техническата експертиза, необходими за ефективното упражняване на техните правомощия, и за вземането на обективни, безпристрастни, и последователни решения“[193].

Съгласно правото на Съвета на Европа – Допълнителният протокол към Конвенция № 108 направи задължително създаването на надзорни органи. В член 1 от този документ се съдържа правната рамка за независимите

193 (ОИСР) (2013 г.) Насоки, уреждащи защитата на неприкосновеността на личния живот и трансграничните потоци от лични данни, точка 19, буква в).

надзорни органи, която договарящите се страни, трябва да приложат в своето национално законодателство. За описанието на задачите и правомощията на тези органи той използва подобни формулировки, като заложенитев Директивата за защита на личните данни. Следователно, надзорните органи следва по принцип да функционират по един и същи начин съгласно правото на ЕС и това на Съвета на Европа.

Съгласно правото на ЕС – компетентностите и организационната структура на надзорните органи бяха описани за първи път в член 28, параграф 1 от Директивата за защита на личните данни. Регламентът относно защитата на данните при обработването им от институции на ЕС[194] определя Европейския надзорен орган по защита на данните (ЕНОЗД) като надзорен орган по отношение на обработването на данни от органите и институциите на ЕС. Когато описва ролите и отговорностите на надзорния орган, регламентът се основава на придобития след обнародването на Директивата за защита на личните данни опит.

Независимостта на органите за защита на данните е гарантирана по силата на член 16, параграф 2 от ДФЕС и на член 8, параграф 3 от Хартата. В последната разпоредба упражняваният, от независим орган, контрол изрично се разглежда като съществен елемент от основното право на защита на личните данни. В допълнение, Директивата за защита на личните данни изисква от държавите членки да установят контролни органи, които да следят за прилагането на директивата, като действат напълно независимо[195]. Освен че законът за създаване на надзорен орган трябва да съдържа разпоредби, които изрично да гарантират неговата независимост, конкретната организационна структура на институцията също трябва да показва неговата самостоятелност.

През 2010 г. Съдът на ЕС за първи път разгледа въпроса за обхвата на изискването за независимост на надзорните органи за защита на данните[196]. Примерите по-долу илюстрират неговите разсъждения.

194 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г., членове 41–48.

195 Директива за защита на личните данни, член 28, параграф 1, последно изречение; Конвенция № 108, Допълнителен протокол, член 1, параграф 3.

196 Вж. FRA (2010 г.), *Основни права: трудности и постижения през 2010 г.*, Годишен доклад за 2010 г., стр. 59. FRA разгледа този въпрос по-подробно в доклада си, озаглавен *„Защита на данните в Европейския съюз: ролята на националните органи за защита на данните“*, който бе публикуван през май 2010 г.

Пример: В делото *Комисия/Германия*[197] Европейската комисия е поискала от Съда на ЕС да обяви, че Германия е транспонирала неправилно изискването за пълна независимост на надзорните органи, отговорни да гарантират защитата на данните, и по този начин не е изпълнила задълженията си по силата на член 28, параграф 1 от Директивата за защита на личните данни. Според Комисията проблемът е бил в това, че Германия е поставила под държавен надзор органите, които са отговорни да следят обработването на личните данни извън публичния сектор в различните федерални провинции (*Länder*).

Според Съда оценката на същността на жалбата зависи от обхвата на изискването за независимост, което се съдържа в разпоредбата, и следователно от нейното тълкуване.

Съдът е подчертал, че думите „с пълна независимост" в член 28, параграф 1 от директивата трябва да се тълкуват въз основа на реалната формулировка на тази разпоредба и в съответствие с целите и механизмите на Директивата за защита на личните данни[198]. Съдът е подчертал, че надзорните органи са „пазители" на правата, свързани с обработването на личните данни, които са гарантирани в директивата, и следователно тяхното създаване в държавите членки се счита за „съществен елемент от защитата на лицата при обработването на лични данни"[199]. Съдът е заключил, че „при упражняване на техните функции надзорните органи трябва да действат обективно и безпристрастно. За целта те трябва да бъдат предпазени от всяко външно влияние, включително от прякото или косвено влияние от страна на държавата или на провинциите, а не само от влиянието на контролираните организации"[200].

Съдът на ЕС е счел също, че значението на термина „пълна независимост" следва да се тълкува с оглед на независимостта на ЕНОЗД, както е определена в Регламента относно защитата на данните при обработването им от институции на ЕС. Както Съдът е подчертал, член 44, параграф 2 от регламента изяснява концепцията за независимост, като допълва, че

197 Съд на ЕС, Решение от 9 март 2010 г. по дело *Европейска комисия/Федерална република Германия*, C-518/07, точка 27.

198 *Пак там*, точки 17 и 29.

199 *Пак там*, точка 23.

200 *Пак там*, точка 25.

„при изпълнение на своите задължения ЕНОЗД не търси и не получава инструкции от никого“. Тези правила изключват намесата на държавен орган, който да упражнява надзор върху независимия орган за защита на данните[201].

В съответствие с това Съдът на ЕС е постановил, че германските институции за защита на данните на федерално равнище, които отговарят за проследяването на обработването на личните данни от непубличните органи, не са достатъчно независими, тъй като са обект на надзор от страна на държавата.

Пример: В делото *Комисия/Австрия*[202] Съдът на ЕС посочва наличието на сходни проблеми, свързани с позицията на някои членове и сътрудници на австрийския орган по защита на данните (Комисията за защита на данните, DSK). В този случай Съдът е заключил, че австрийското законодателство не позволява на австрийския орган за защита на данните да изпълнява задачите си при пълна независимост по смисъла на Директивата за защита на личните данни. Независимостта на австрийския орган за защита на данните не е гарантирана в достатъчна степен, тъй като Федералното канцлерство подсигурява персонала на DSK, упражнява надзор на дейността на DSK и има право да бъде информирано по всяко време за нейната работа.

Пример: *Европейската комисия с/у Унгария*[203], СЕС обърна внимание, че „изискването [...] да се гарантира,че всеки надзорен орган е в състояние да извършва дейностите, които са му възложени в пълна независимост, съдържа задължение за съответните страни членки да позволят реализирането на пълен мандат на органа.“ Съдът също така счита, че „с предсрочното прекратяване на мандата на надзорния орган за защита на данните, Унгария не е изпълнила задълженията си по Директива 95/46/ЕО[...].“

201 *Пак там*, точка 27.

202 Съд на ЕС, Решение от 16 октомври 2012 г. по дело *Европейска комисия/Република Австрия*, C-614/10, точки 59 и 63.

203 Съд на ЕС, C-288/12, *Европейската комисия с/у Унгария*, 8 април 2014 г., параграфи 50 and 67

Съгласно националното законодателство надзорните органи разполагат с правомощия и компетентност, наред с другото[204]:

- да съветват администраторите и физическите лица по всички въпроси, свързани със защитата на данните;
- да разследват операциите по обработване и да се намесват по подходящ начин;
- да отправят предупреждения или строги забележки към администраторите;
- да разпореждат коригиране, блокиране, изтриване или унищожаване на данни;
- да налагат временна или окончателна забрана за обработване;
- да сезират съда по конкретни случаи.

За да може да изпълнява задълженията си, надзорният орган трябва да има достъп до всички лични данни и до цялата информация, необходима за провеждане на разследване, както и до местата, в които даден администратор съхранява съответната информация.

Съществуват значителни различия между отделните местни юрисдикции по отношение на процедурите и правните действия, произтичащи от констатациите на надзорните органи. Те могат да варират от препоръки, подобни на тези, които прави омбудсманът, до незабавно изпълними решения. Поради това, когато се анализира ефективността на средствата за защита, които са налични в рамките на дадена юрисдикция, те трябва да бъдат оценявани в съответния контекст.

204 Директива за защита на личните данни, член 28; вж. освен това Конвенция № 108, Допълнителен протокол, член 1.

5.3. Средства за правна защита и санкции

Ключови въпроси

- Съгласно Конвенция № 108, както и Директивата за защита на личните данни, в националното законодателство трябва да се определят подходящи средства за правна защита и санкции срещу нарушенията на правото на защита на данните.
    - Съгласно правото на ЕС, правото на ефективна правна защита изисква в националното законодателство да се определят средства за правна защита срещу нарушения на правата, свързани със защитата на данните, независимо от възможността за сезиране на надзорния орган.
    - Санкциите трябва да бъдат определени от националното законодателство и да бъдат ефективни, равностойни, пропорционални и възпиращи.
- Преди да се обърне към съда, лицето трябва най-напред да сезира администратора. От разпоредбите на съответното национално законодателство зависи доколко е задължително или не да се сезира надзорният орган преди подаването на жалба в съда.
- При определени условия физическите лица могат да подават оплаквания, свързани с нарушения на законодателството за защита на данните, пред Европейския съд по правата на човека в качеството му на последна инстанция.
- В допълнение физическите лица могат да се обръщат към Съда на ЕС, но само в много ограничена степен.

Правата по силата на законодателството за защита на данните могат да се упражняват само от лицето, чиито права са изложени на риск; това трябва да е някой, който е или поне претендира да е съответното физическо лице. При упражняването на своите права такова лице може да бъде представлявано от лица, които изпълняват необходимите изисквания по силата на националното законодателство. Непълнолетните лица трябва да бъдат представлявани от своите родители или настойници. Пред надзорните органи дадено физическо лице може да бъде представлявано също и от асоциации, чиято законна цел е да насърчават правата, свързани със защитата на данните.

5.3.1. Искане, отправено към администратора

Правата, посочени в раздел 3.2, трябва най-напред да бъдат упражнени пред администратора. Прякото сезиране на националния надзорен орган или на съда не би било от полза, тъй като органът би могъл само да даде препоръка,

че оплакването трябва най-напред да бъде адресирано към администратора, а съдът би определил молбата за недопустима. Формалните изисквания за правно допустимо искане към администратор, особено изискването дали искането трябва да е писмено, следва да бъдат определени от националното законодателство.

Субектът, който е бил сезиран в качеството на администратор, трябва да реагира на искането, дори да не е реалният администратор. Отговорът трябва във всеки случай да бъде предоставен на физическото лице в рамките на срока, определен от националното законодателство, дори ако в него просто се казва, че не се обработват данни относно лицето, отправило искането. В съответствие с разпоредбите на член 12, буква а) от Директивата за защита на личните данни и на член 8, буква б) от Конвенция № 108 подобно искане трябва да бъде разгледано „без прекалено забавяне". Следователно националното законодателство следва да предвиди срок за отговор, който да е достатъчно кратък, като в същото време дава възможност на администратора да разгледа искането по подходящ начин.

Преди да отговори на искането субектът, който е бил сезиран в качеството на администратор, трябва да установи самоличността на лицето, отправило искането, за да определи дали то действително е лицето, за което се представя, и по този начин да предотврати сериозно нарушение на изискванията за поверителност. Когато изискванията за установяване на самоличността не са изрично определени в националното законодателство, те трябва да бъдат определени с решение на администратора. Принципът за добросъвестно обработване обаче изисква администраторите да не налагат прекалено тежки условия за установяване на самоличността (както и за автентичността на запитването, както бе обсъдено в раздел 2.1.1).

Също така в националното законодателство трябва да се реши въпросът дали администраторите могат, преди да отговорят на исканията, да поискат заплащането на такса от лицето, отправило искането, или не: в член 12, буква а) от директивата и член 8, буква б) от Конвенция № 108 се предвижда, че отговорът на запитване за достъп трябва да бъде даван без прекалени разходи. Националното законодателство в много европейски държави предвижда на исканията, свързани съсзащитата на данните да се отговаря безплатно, доколкото отговорът не налага прекомерни и необичайни усилия; от своя страна, националното законодателство обикновено защитава администраторите срещу злоупотреби с правото на получаване на отговор на искане.

Ако лицето, институцията или органът, които са били сезирани в качеството на администратори, не отрича, че е администратор на данните, то в предвидения от националното законодателство срок той трябва:

- да уважи искането и да уведоми лицето как искането му е било изпълнено; или

- да уведоми лицето, отправило искането, защо неговото искане няма да бъде уважено.

5.3.2. Жалби, подадени до надзорния орган

Когато лице, след като е подало искане за достъп или е направило възражение пред администратор, не получи своевременен и задоволителен отговор, то може да се обърне към националния надзорен орган за защита на данните с искане за помощ. В хода на производството пред надзорния орган следва да се изясни дали лицето, институцията или органът, към които се е обърнало лицето, отправило искането, действително е бил задължен да реагира на искането или не, и дали неговата реакция е била правилна и достатъчна. Надзорният орган трябва да уведоми засегнатото лице относно резултата от производствата по неговия иск[205]. Правните последици, свързани с резултата от производствата пред националния надзорен орган, зависят от националното законодателство: дали решенията на органа могат да бъдат законно изпълнени, т.е. дали те могат да бъдат приложени от официален орган или е необходимо да се сезира съдът, в случай че администраторът не изпълнява решенията (становище, строга забележка и т.н.) на надзорния орган.

В случай че съществува твърдение за нарушение на правата, свързани със защита на данните, гарантирани съгласно член 16 от ДФЕС, от страна на институции или органи на ЕС, физическото лице може да подаде жалба пред ЕНОЗД[206] — независимият надзорен орган зазащита на личните данни съгласно Регламента относно защитата на данните при обработването им от институции на ЕС, който определя задълженията и правомощията на ЕНОЗД. При липса на отговор от ЕНОЗД в срок от шест месеца, жалбата се счита за отхвърлена.

205 Директива за защита на личните данни, член 28, параграф 4.

206 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г.

Трябва да съществува възможност за обжалване на решението на национален надзорен орган пред съда. Това се отнася както за физическите лица, така и за администраторите, които са били страна по производства пред съответния контролен орган.

Пример: На 24 юли 2013 г. комисарят по информацията на Обединеното кралство излезе с решение, с което иска от полицията в Хердфоршир да престане да използва, считаната за незаконна, система за проследяване на табелите на превозните средства. Данните, събрани от камерите, са запазени както в базата данни на местната полиция, така и в централизирана база данни. Лицензираните снимки на табелите на автомобилите се съхраняват за срок от две години, а снимките на колите — в продължение на 90 дни. Беше счетено, че подобна широка употреба на камери и други форми за наблюдение не е пропорционална на проблема, който тя се опитва да реши.

5.3.3. Жалби, подадени пред съда

Съгласно Директивата за защита на личните данни, ако лице, подало искане до администратор във връзка съсзащита на данните, не е удовлетворено от отговора на този администратор, това лице трябва да има право да внесе жалба пред национален съд[207].

От разпоредбите на съответното национално законодателство зависи доколко е задължително или не първо да се сезира надзорният орган преди подаването на жалба в съда. В повечето случаи обаче за лицата, упражняващи своите права зазащита на данните, би било по-добре да се обърнат най-напред към надзорния орган, тъй като неговата помощ при разглеждането на искове следва да бъде облекчена от гледна точка на бюрократичните процедури и да е безплатна. Експертната оценка, документирана в решението на надзорния орган (становище, строга забележка и т.н.), може също така да помогне на физическото лице да защити правата си в съда.

Съгласно правото на Съвета на Европа твърденията за нарушения на правата в областта на защитата на данните на национално равнище в договаряща се страна по ЕКПЧ, които в същото време представляват нарушение на член 8

207 Директива за защита на личните данни, член 22.

от ЕКПЧ, могат допълнително да бъдат внасяни в ЕСПЧ след изчерпване на всички достъпни средства за правна защита на национално равнище. Внасянето на жалба за нарушение на член 8 от ЕКПЧ пред ЕСПЧ трябва също така да отговаря и на други критерии за допустимост (членове 34—37 от ЕКПЧ)[208].

Въпреки че молбите до ЕСПЧ могат да се отнасят единствено до държави, които са договарящи се страни по конвенцията, те могат частично да касаят действия или бездействия на частни лица, доколкото договарящата се страна по конвенцията, не е изпълнила задълженията си по силата на ЕКПЧ и не е предоставила в своето национално законодателство достатъчна защита срещу нарушения на правата за на защита на личните данни.

Пример: В делото *K.U./Финландия*[209] жалбоподателят, непълнолетно лице, се е жалвал от реклама със сексуален характер с негово участие, публикувана в интернет сайт за запознанства. Самоличността на лицето, публикувало информацията, не е била разкрита от доставчика на сървъра заради ангажиментите за поверителност, които се налагат от финландското законодателство. Жалбоподателят твърдял, че финландското законодателство не предоставя достатъчна защита срещу подобни действия на частното лице, публикувало уличаващи данни относно жалбоподателя в интернет. ЕСПЧ е постановил, че държавите не само са длъжни да се въздържат от произволна намеса в личния живот на хората, но имат и позитивни задължения, които включват „приемането на мерки, насочени да гарантират зачитането на неприкосновеността на личния живот дори в отношенията на лицата между самите тях". В случая на жалбоподателя неговата практическа и ефективна защита изисква предприемането на ефективни мерки за идентифицирането и наказателното преследване на извършителя. Такава защита обаче не е била предприета от държавата и Съдът излиза със заключение, че в този случай е налице нарушение на член 8 от ЕКПЧ.

Пример: В делото *Köpke/Германия*[210] жалбоподателката е била заподозряна в извършване на кражба на работното си място и по тази причина е била подложена на скрито видеонаблюдение. ЕСПЧ е заключил, че

208 ЕКПЧ, членове 34—37, достъпна на адрес: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 ЕСПЧ, Решение от 2 март 2009 г. по дело *K.U./Финландия*, № 2872/02.

210 ЕСПЧ, Решение от 5 октомври 2010 г. по дело *Köpke/Германия* (dec.), № 420/07.

„нищо не сочи, че местните органи не са успели да осигурят подходящ баланс, в рамките на своята възможност за преценка, между правото на зачитане на неприкосновеността на личния живот на жалбоподателката съгласно член 8, от една страна, и интереса на работодателя да защити своите права на собственост и обществения интерес, свързан с доброто правораздаване, от друга страна“. Поради това молбата е била обявена за недопустима.

Ако ЕСПЧ постанови, че държава — страна по конвенцията, е нарушила някое от правата, защитени от ЕКПЧ, държавата — страна по конвенцията, е длъжна да изпълни решението на ЕСПЧ. Мерките за изпълнение трябва на първо място да прекратяват нарушението и да отстраняват, доколкото това е възможно, негативните последици за жалбоподателя. Изпълнението на решенията може да изисква също прилагането на общи мерки за предотвратяване на нарушения, подобни на установените от Съда, било чрез промяна в законодателството, съдебна практика или други мерки.

В член 41 от ЕСПЧ се предвижда, че когато ЕСПЧ установи нарушение на ЕКПЧ, той може да постанови справедливо обезщетение за ищеца за сметка на държавата — страна по конвенцията.

Съгласно правото на ЕС[211] жертвите на нарушения на националното законодателство за защита на данните, чрез което се прилага правото на ЕС в областта на защитата на данните, могат в някои случаи да се обърнат към Съда на ЕС. Има два възможни сценария за начина, по който жалбата на физическо лице, свързана с нарушение на неговите права в областта на защитата на данните, може да доведе до производство пред Съда на ЕС.

При първия сценарий физическото лице трябва да е пряка жертва на административен или нормативен акт на ЕС, който нарушава правото на лицето на защита на неговите данни. Съгласно член 263, параграф 4 от ДФЕС:

„Всяко физическо или юридическо лице може да заведе иск [...] срещу решенията, които са адресирани до него или които го засягат пряко

211 ЕС (2007 г.), Договор от Лисабон за изменение на Договора за Европейския съюз и на Договора за създаване на Европейската общност, подписан в Лисабон, 13 декември 2007 г., ОВ C 306, 17.12.2007 г. Вж. също консолидираните текстове на Договора за Европейския съюз, ОВ C 326, 26.10.2012 г. и на Договора за функционирането на Европейския съюз, ОВ C 326, 26.10.2012 г.

и лично, както и срещу подзаконови актове, които го засягат пряко и които не включват мерки за изпълнение."

Така жертвите на незаконно обработване на личните им данни от орган на ЕС могат да се обърнат директно към Общия съд на Съда на ЕС, който е органът, разполагащ с правомощия да взема решения по въпроси, свързани с Регламента относно защитата на данните при обработването им от институции на ЕС. Възможността за пряко сезиране на Съда на ЕС съществува също и в случаите, когато нечий правен статут е пряко засегнат от правна разпоредба на ЕС.

Вторият сценарий е свързан с правомощието на Съда на ЕС да дава преюдициални заключения в съответствие с член 267 от ДФЕС.

В хода на производство на национално равнище дадено физическо лице може да поиска от националния съд да изиска разяснение от Съда на ЕС относно тълкуването на Договорите на ЕС и относно тълкуването и действителността на актове на институции, органи, служби или агенции на ЕС. Подобни разяснения се наричат преюдициални заключения. Те не предлагат пряка правна защита на жалбоподателя, но позволяват на националните съдилища да гарантират, че прилагат правилното тълкуване на правото на ЕС.

Ако една от страните в производство пред национален съд поиска да се отправи запитване до Съда на ЕС, с това са длъжни да се съобразят само националните съдилища, които действат като последна инстанция и чиито решения не подлежат на съдебно обжалване.

Пример: В делото *Kärntner Landesregierung и други*[212] Конституционният съд на Австрия отправя запитване до Съда на ЕС относно действителността на членове 3—9 от Директива 2006/24/ЕО (*Директивата за запазване на лични данни*) с оглед на членове 7, 9 и 11 от Хартата и относно това дали някои разпоредби на австрийския федерален закон за далекосъобщенията, който транспонира Директивата за запазване на лични данни, са несъвместими с елементи от Директивата за защита на личните данни и с Регламента относно защитата на данните при обработването им от институции на ЕС.

212 Съд на ЕС, Съединени дела C-293/12 и C-594/12, *Digital Rights Ireland и Seitling и Others*, 8 април 2014 г.

Г-н Seitlinger, един от жалбоподателите по производството пред конституционния съд, заявява, че използва телефона, интернет и електронната си поща както за служебни цели, така и в личния си живот. Следователно информацията, която изпраща и получава, минава през обществени далекосъобщителни мрежи. По силата на австрийския закон за далекосъобщенията от 2003 г. неговият доставчик на далекосъобщителни услуги има законово задължение да събира и съхранява данни относно начина, по който той използва мрежата. Г-н Seitlinger разбира, че това събиране и съхранение на личните му данни по никакъв начин не е технически необходимо за пренасянето на информацията от точка А до точка Б в мрежата. Събирането и съхранението на тези данни не е необходимо дори за целите на фактурирането. Г-н Seitlinger със сигурност не е дал съгласието си за използването на личните му данни по такъв начин. Единствената причина за събирането и съхранението на всички тези допълнителни данни е австрийският закон за далекосъобщенията от 2003 г.

Поради това г-н Seitlinger е подал жалба пред австрийския конституционен съд, в която твърди, че законовите задължения на неговия доставчик на далекосъобщителни услуги нарушават основните му права по член 8 от Хартата на ЕС.

Съдът на ЕС излиза с решение само относно основните елементи на горепосоченото искане за преюдициално заключение. Националният съд запазва своята компетентност да излезе с решение по изходното дело.

По принцип Съдът на ЕС трябва да отговори на въпросите, които са му отправени. Той не може да откаже да даде преюдициално заключение с аргумента, че отговорът няма да е съотносим спрямо изходното дело, нито своевременен. Въпреки това той може да откаже, ако въпросът не попада в обхвата на неговата компетентност.

Накрая, ако съществува твърдение за нарушение на правата, свързани със защитата на данните, гарантирани съгласно член 16 от ДФЕС, от институция или орган на ЕС в хода на обработването на лични данни, физическото лице може да внесе жалба пред Общия съд на Съда на ЕС (член 32, параграфи 1 и 4 от Регламента относно защитата на данните при обработването им от институции на ЕС). Същото се отнася и до решенията на ЕНОЗД относно подобни нарушения (член 32, параграф 3 от Регламента относно защитата на данните при обработването им от институции на ЕС).

Въпреки че Съдът на ЕС е компетентен да се произнася по случаи, свързани с Регламента относно защитата на данните при обработването им от институции на ЕС, ако дадено лице иска правна защита в качеството си на служител в институция или орган на ЕС, то трябва да се обърне към Съда на публичната служба на ЕС.

Пример: Делото *Европейска комисия/The Bavarian Lager Co. Ltd*[213] показва достъпните средства за правна защита срещу действия или решения на институциите и органите на ЕС, свързани със защитата на данните.

Bavarian Lager е поискало от Европейската комисия достъп до пълния протокол от събрание, организирано от Комисията, за което се твърди, че се отнася до правни въпроси, свързани с дружеството. Комисията е отхвърлила искането за достъп на дружеството по съображения за преимуществени интереси, свързани със защитата на данните[214]. В приложение на член 32 от Регламента относно защитата на данните при обработването им от институции на ЕС Bavarian Lager е подало жалба срещу това решение пред Съда на ЕС; по-точно пред Първоинстанционния съд (предшественикът на Общия съд). Със своето решение по дело T-194/04, *Bavarian Lager/Комисия*, Първоинстанционният съд е отменил решението на Комисията да отхвърли искането за достъп. Европейската комисия е обжалвала това решение на Съда на ЕС. Съдът е постановил решение (в разширен състав), с което е отменил решението на Първоинстанционния съд и потвърдил отказа на Европейската комисия да удовлетвори искането за достъп.

5.3.4. Санкции

Съгласно правото на Съвета на Европа — член 10 от Конвенция № 108 предвижда, че „всяка страна се задължава да установи съответстващи санкции и компенсации при нарушаване на разпоредбите на вътрешното право, с които се въвеждат в действие принципите за защита на данните, залегнали

213 Съд на ЕС, Решение от 29 юни 2010 г. по дело *Европейска комисия/The Bavarian Lager Co. Ltd*.

214 За анализ на спора, вж.: ЕНОЗД (2011 г.), *Публичен достъп до съдържащи лични данни документи след решението по делото Bavarian Lager*, Брюксел, ЕНОЗД, достъпно на адрес: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964.

в Конвенция № 108[215]. **Съгласно правото на ЕС** — в член 24 от Директивата за защита на личните данни се постановява, че държавите членки „вземат подходящи мерки, за да гарантират пълното прилагане на разпоредбите на настоящата директива и в частност определят санкциите, които се налагат в случай на нарушаване на разпоредбите, приети [...]".

И двата инструмента оставят на държавите членки свобода на преценка при избора на подходящите санкции и компенсации. Нито един от правните инструменти не предлага специфични насоки относно същността или вида на подходящите санкции, нито дава примери за санкции.

Въпреки това:

> *„въпреки че държавите членки на ЕС, се ползват от свобода на преценка при определянето на най-подходящите мерки за защита на правата, които правните субекти черпят от правото на ЕС, в съответствие с принципа за лоялно сътрудничество, предвиден в член 4, параграф 3 от ДЕС, минималните изисквания за ефективност, равностойност, пропорционалност и възпиращ ефект следва да бъдат спазени"*[216].

Съдът на ЕС неведнъж е поддържал становището, че националното законодателство не е напълно свободно при определянето на санкциите.

Пример: В делото *Von Colson и Kamann/Land Nordrhein-Westfalen*[217] Съдът на ЕС посочи, че всички държави членки, към които е насочена дадена директива, са длъжни да предприемат в своите правни системи всички необходими мерки, за да гарантират, че тя се прилага ефективно в съответствие с целите, които преследва. Съдът е постановил, че въпреки че държавите членки избират начините и средствата за гарантиране на прилагането на директивата, тази свобода не засяга задължението,

215 ЕСПЧ, Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03; ЕСПЧ, Решение от 2 декември 2008 г. по дело *K.U/Финландия*, № 2872/02.

216 FRA (2012 г.), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, 2/2012 [Становище 2/2012 на Агенцията на Европейския съюз за основните права относно предложения пакет от реформи за защита на данните]*, Виена, 1 октомври 2012 г., стр. 27.

217 Съд на ЕС, C-14/83, *Sabine von Kolson и Elisabeth Kamann с/у провинция Северен Рейн- Вестфалия*, 10 април 1984 г.

което им е наложено. По-специално, ефективното средство за правна защита трябва да позволява на правния субект да преследва и да налага спазването на въпросното право в пълна степен. За постигането на тази реална и ефективна защита, средствата за правна защита трябва да задействат наказателни и/или компенсаторни процедури, които водят до санкции с възпиращ ефект.

Що се отнася до санкциите за нарушения на правото на ЕС от страна на институции или органи на ЕС, поради специалния обхват на компетентност на Регламента относно защитата на данните при обработването им от институции на ЕС, санкции са предвидени само под формата на дисциплинарни мерки. Съгласно член 49 от регламента „всяко неспазване на задължения съгласно настоящия регламент от страна на служител или друго длъжностно лице на Европейските общности, независимо дали преднамерено или по непредпазливост, води до дисциплинарни санкции [...]".

6

Трансгранични потоци от данни

ЕС	Обхванати въпроси	Съвет на Европа
Трансгранични потоци от данни		
Директива за защита на личните данни, член 25, параграф 1 Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01	Определение	Конвенция № 108, Допълнителен протокол, член 2, параграф 1
Свободни потоци от данни		
Директива за защита на личните данни, член 1, параграф 2	Между държави членки на ЕС	
	Между договарящи се страни по Конвенция № 108	Конвенция № 108, член 12, параграф 2
Директива за защита на личните данни, член 25	Към трети държави с адекватно ниво на защита на данните	Конвенция № 108, Допълнителен протокол, член 2, параграф 1
Директива за защита на личните данни, член 26, параграф 1	Към трети държави в специални случаи	Конвенция № 108, Допълнителен протокол, член 2, параграф 2, буква а)
Ограничен поток от данни към трети държави		
Директива за защита на личните данни, член 26, параграф 2 Директива за защита на личните данни, член 26, параграф 4	Договорни клаузи	Конвенция № 108, Допълнителен протокол, член 2, параграф 2, буква б) Ръководство за изготвянето на договорни клаузи

Директива за защита на личните данни, член 26, параграф 2	**Задължителни корпоративни правила**	
Примери: Споразумение между ЕС и САЩ относно PNR данни Споразумение между ЕС и САЩ относно SWIFT	**Специални международни споразумения**	

Директивата за защита на личните данни не само предвижда свободно движение на данни между държавите членки, но също така съдържа разпоредби относно изискванията за трансфера на лични данни към трети държави извън ЕС. Съветът на Европа също така признава важността на прилагането на правилата за трансгранично движение наданни към трети държави и прие Допълнителния протокол към Конвенция № 108 през 2001 г. Този протокол включи основните регулаторни аспекти по отношение на трансграничните потоци от данни, произхождащи от страните по конвенцията и държавите членки на ЕС.

6.1. Естество на трансграничното предостовяне на данни

Ключов въпрос

- Трансграничното предоставяне на данни представляват трансфер на лични данни към получател, който е обект на чужда юрисдикция.

В член 2, параграф 1 от Допълнителния протокол към Конвенция № 108 трансграничното предоставяне данни е описано като трансфер на лични данни към получател, който е обект на чужда юрисдикция. Член 25, параграф 1 от Директивата за защита на личните данни урежда „предаването на лични данни, които са подложени на обработка или са предназначени за обработка след предаването им на трета страна [...]“. Такова предаване на данни е разрешено само в съответствие с правилата, изложени в член 2 от Допълнителния протокол към Конвенция № 108, а за държавите членки на ЕС — допълнително и в членове 25 и 26 от Директивата за защита на личните данни.

Пример: По делото *Bodil Lindqvist*[218] Съдът на ЕС постанови, че „операция, състояща се в позоваването в интернет страница на различни лица и определянето им или по име, или по друг начин, например чрез телефонен номер или данни, свързани с условията им на работа и развлеченията им, представлява „пълна или частична обработка на лични данни с автоматизирани средства“ по смисъла на член 3, параграф 1 от Директива 95/46/ЕО“.

След това Съдът посочи, че Директивата също така определя специални правила, предназначени да позволят на държавите членки да извършват мониторинг на трансфера на лични данни към трети държави.

Въпреки това обаче, като се има предвид, първо, степента на развитие на интернет към момента на изготвянето на директивата и второ, липсата на критерии в нея, които са приложими по отношение на използването на интернет, не може да се приеме, че „законодателната власт на Общността е предвиждала изразът „предаване [на данни] на трета страна“ да обхваща качването [ ] на данни на интернет страница, дори и да стават достъпни по този начин за лица в трети държави, които имат технически средства за достъп до тях“.

В противен случай, ако директивата е „тълкувана в смисъл, че е налице предаване на данни на трета държава винаги, когато лични данни се качват на интернет страница, това предаване би било по необходимост предаване на всички трети държави, в които са налице необходимите технически средства за достъп до интернет. Специалният, предвиден [от директивата] режим, би се превърнал по необходимост в режим за общо приложение по отношение на операциите в интернет. Така, ако Комисията е установила [...], че дори една трета държава да не е гарантирала достатъчна защита, държавите членки биха били длъжни да възпрепятстват поставянето на всякакви лични данни в интернет.“

Принципът, че самото публикуване на (лични) данни не трябва да се разглежда като трансгранично предаване на данни, се прилага също така по отношение на он-лайн публичните регистри или средствата за масова информация, като (електронни) вестници и телевизия. Само съобщение, което е насочено към конкретни получатели, има отношение към понятието „трансгранично предаване на данни“.

218 Съд на ЕС, Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01, точки 27, 68 и 69.

6.2. Свободно движение на данни между държавите членки или между договарящите се страни

Ключов въпрос

- Трансферът на лични данни към друга държава членка на Европейското икономическо пространство, или към друга договаряща се страна по Конвенция № 108 трябва да бъде освободен от ограничения.

Съгласно правото на Съвета на Европа — член 12, параграф 2 от Конвенция № 108 — трябва да е налице свободно движение на лични данни между страните по конвенцията. Националното законодателство не може да ограничава изнасянето на лични данни към дадена договаряща се страна освен ако:

- специфичното естество на данните изисква това[219]; или
- ограничението е необходимо, за да се избегне заобикалянето на националните правни разпоредби относно трансграничното предаване на данни към трети лица[220].

Съгласно правото на ЕС ограниченията или забраните на свободното движение на лични данни между държавите членки по съображения, свързани със защитата на данните, са забранени в член 1, параграф 2 от Директивата за защита на личните данни. Зоната на свободното движение на данни е разширена със Споразумението за Европейското икономическо пространство (ЕИП)[221], с което Исландия, Лихтенщайн и Норвегия се включват във вътрешния пазар.

Пример: Ако съдружник в международна група от дружества, установени в няколко държави членки на ЕС, сред които Словения и Франция,

219 Конвенция № 108, член 12, параграф 3, буква а).

220 *Пак там*, член 12, параграф 3, буква б).

221 Решение на Съвета и на Комисията от 13 декември 1993 г. за сключване на Споразумението за Европейското икономическо пространство между Европейските общности, техните държави членки и Република Австрия, Република Финландия, Република Исландия, Княжество Лихтенщайн, Кралство Норвегия, Кралство Швеция и Конфедерация Швейцария, ОВ L 1, 3.1.1994 г.

предава лични данни от Словения на Франция, подобен поток от данни не трябва да се ограничава или забранява от словенското национално законодателство.

Ако обаче същият словенски съдружник иска да предаде същите лични данни на дружеството майка в САЩ, словенският износител на данни трябва да премине през процедурите, установени в словенското законодателство за трансгранично предоставяне на данни към трети държави без адекватна защита на данните, освен ако дружеството майка не се е присъединило към принципите за „гарантиране на неприкосновеност на личния живот" — доброволен кодекс за поведение, с който се осигурява адекватно ниво на защита на данните (вж. раздел 6.3.1).

Трансграничното прехвърляне на данни към държави членки на ЕИП, за цели извън обхвата на вътрешния пазар, като например за разследване на престъпления, обаче не подлежат на разпоредбите на Директивата за защита на личните данни и следователно не са обхванати от принципа за свободно движение на данни. Що се отнася до правото на Съвета на Европа, всички области са включени в обхвата на Конвенция № 108 и Допълнителния протокол към Конвенция № 108, въпреки че договарящите се страни могат да правят изключения. Всички членове на ЕИП са също и страни по Конвенция № 108.

6.3. Свободно предоставяне наданни към трети държави

Ключови въпроси

- Трансферът на лични данни към трети държави се извършва без ограничения съгласно националното право в областта на защитата на данните, ако:
  - е била установена адекватността на защитата на данните при получателя; или
  - това е необходимо с цел да се отговори на специфичните интереси на физическото лице или на законните преимуществени интереси на други лица, особено на важни обществени интереси.
- Адекватността на защитата на данните в трета държава означава, че основните принципи на защита на данните са били приложени ефективно в националното законодателство на тази държава.

- Съгласно правото на ЕС адекватността на защитата на данните в трета държава се оценява от Европейската комисия. Съгласно правото на Съвета на Европа определянето на начина, по който се оценява адекватността, е оставено на националното законодателство.

6.3.1. Свободно прехвърляне на данни вследствие на адекватна защита

Правото на Съвета на Европа позволява националното законодателство да дава възможност за свободно движение на данни към държави, които не са страни по конвенцията, ако държавата или организацията получател осигурява адекватно ниво на защита за планирания трансфер на данни[222]. В националното законодателство се определя начинът на оценяване на нивото на защита на данните в чужда държава, както и кой следва да оценява това ниво.

Съгласно правото на ЕС свободното движение наданни към трети държави с адекватно ниво на защита на данните е предвидено в член 25, параграф 1 от Директивата за защита на личните данни. Изискването за адекватност, вместо за равностойност, прави възможно признаването на различни начини за осъществяването на защитата на данните. Съгласно член 25, параграф 6 от директивата Европейската комисия е компетентна да оценява нивото на защита на данните в чужди държави чрез констатиране на адекватността, като се консултира по въпроса за оценяването с Работната група по член 29, която е допринесла в значителна степен за тълкуването на членове 25 и 26[223].

Направената от Европейската комисия констатация за адекватност има обвързващ ефект. Ако Европейската комисия публикува констатация за адекватност в *Официален вестник на Европейския съюз*, всички държави членки

222 Конвенция № 108, Допълнителен протокол, член 2, параграф 1.

223 Вж. например Работна група за защита на личните данни по член 29 (2003 г.), *Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers [Работен документ относно трансфера на лични данни към трети държави: прилагане на член 26, параграф 2 от Директивата на ЕС за защита на личните данни по отношение на задължителните корпоративни правила за международен трансфер на данни]*, WP 74, Брюксел, 3 юни 2003 г.; и Работна група за защита на личните данни по член 29 (2005 г.), *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995 [Работен документ за общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г.]*, WP 114, Брюксел, 25 ноември 2005 г.

на ЕИП, и техните органи са задължени да спазват решението, което означава, че движението на данни към тази държава е възможно без провеждането на процедури по проверяване или лицензиране от национални органи[224].

Освен това, Европейската комисия може да оценява части от правната система на дадена държава или да се ограничи до единични теми. Например, Комисията е направила констатация за адекватност, която касае само и единствено законодателството за частна търговия в Канада[225]. Освен това съществуват и няколко решения за адекватност, свързани с трансфери на данни, въз основа на споразумения между ЕС и чужди държави. Тези решения се отнасят единствено за еднократни трансфери на данни, каквито са предаването на резервационни данни на пътниците от авиокомпаниите към чуждестранните органи за граничен контрол, когато авиокомпанията осъществява полети от ЕС до определени отвъдморски дестинации (вж. раздел 6.4.3). По-скорошната практика на трансфер на данни, въз основа на специално споразумение между ЕС и трети държави, в повечето случаи не включва необходимостта от констатиране на адекватността, като се допуска, че самото споразумение осигурява адекватно ниво на защита на данните[226].

Едно от най-важните решения относно адекватността, в действителност, не е свързано с набор от правни разпоредби[227]. По-скоро то засяга правила като кодекс за поведение, известен под наименованието принципи за „гарантиране на неприкосновеност на личния живот“ (Safe Harbour). Тези принципи са

224 За постоянно актуализиран списък на държавите, които са получили констатация за адекватност, вж. интернет страницата на Генерална дирекция „Правосъдие“ на Европейската комисия, достъпен на адрес: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 Европейска комисия (2012 г.), Решение 2002/2/ЕО на Комисията от 20 декември 2001 г. относно констатиране съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета нивото на адекватна защита на личните данни, осигурявано от канадския закон за защита на личните данни и електронните документи, ОВ L 2, 4.1.2002 г.

226 Например Споразумението между Съединените американски щати и Европейския съюз относно използването и предаването на резервационни данни на пътниците на Министерството на вътрешната сигурност на Съединените щати (ОВ L 215, 11.8.2012 г., стр. 5—14) или Споразумението между Европейския съюз и Съединените американски щати относно обработката и изпращането на данни за финансови съобщения от Европейския съюз до Съединените Американски щати за целите на програмата за проследяване на финансирането на тероризма, ОВ L 8, 13.1.2010 г., стр. 11–16.

227 Европейска комисия (2012 г.), Решение 2000/520/ЕО на Комисията от 26 юли 2000 г. съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, гарантирана от принципите за „сфера на неприкосновеност на личния живот“ и свързаните с това често задавани въпроси, публикувани от Департамента по търговия на САЩ, ОВ L 215, 25.8.2000 г.

били разработени между ЕС и САЩ за търговските дружества в САЩ. Членството в тази програма се постига чрез доброволно поемане на ангажимент, декларирано пред Министерството на търговията на САЩ и документирано в списък, който се публикува от това министерство. Един от важните елементи на адекватността е ефективното осъществяване на защита на данните, като Споразумението за гарантиране на неприкосновеността също така предвижда надзор от държавата в определена степен: в програмата могат да се включат само онези дружества, които подлежат на контрол от Федералната комисия по търговия на САЩ.

6.3.2. Свободно движение на данни в специални случаи

Съгласно правото на Съвета на Европа — член 2, параграф 2 от Допълнителния протокол към Конвенция № 108 дава възможност за трансфера на лични данни към трети държави, в които не е налице адекватна защита на данните, при условие че трансферът е предвиден в националното законодателство и е необходим за:

- специфични интереси на съответното физическо лице; или
- законни преимуществени интереси на други лица, по-специално важни обществени интереси.

В рамките на правото на ЕС — член 26, параграф 1 от Директивата за защита на личните данни съдържа разпоредби, които са сходни с тези на Допълнителния протокол към Конвенция № 108.

Съгласно директивата интересите на съответното физическо лице могат да обосноват свободното движение на данни към трета държава, ако:

- съответното физическо лице е дало своето недвусмислено съгласие за изнасянето на данните; или
- съответното физическо данни влиза във — или се подготвя да влезе — в договорни отношения, които ясно изискват трансфер на данните на получател в чужбина; или

- е сключен договор между администратор на данни и трето лице, който е в интерес на съответното физическо лице; или

- трансферът е необходим за защита на жизненоважните интереси на физическото лице.

- за трансфера на данни от публични регистри; това е пример за преимуществените интереси на обществеността, за да може да има достъп до информацията, съхранявана в публичните регистри.

Законните интереси на други лица могат да обосноват свободното трансгранично движение на данни[228]:

- поради важен обществен интерес, различен от въпроси, свързани с националната или обществена сигурност, тъй като те не попадат в обхвата на Директивата за защита на личните данни; или

- с цел предявяване, изпълнение или защита на правни искове.

Разгледаните по-горе случаи трябва да бъдат разбирани като изключения от правилото, което гласи, че свободният трансфер на данни към други държави изисква адекватно ниво на защита на данните в държавата получател. Изключенията трябва винаги да се тълкуват ограничително. Това е застъпвано многократно от Работната група по член 29 в контекста на член 26, параграф 1 от Директивата за защита на личните данни, особено, когато съгласието е предполагаемото основание за трансфер на данни[229]. Работната група по член 29 е направила заключение, че общите правила относно правната значимост на съгласието се прилагат също така и спрямо член 26, параграф 1 от директивата. Ако например в контекста на трудови отношения не е ясно дали съгласие, дадено от служители, е действително свободно изразено съгласие, трансферите на данни не могат да се основават на член 26, параграф 1 от директивата. В тези случаи приложим е член 26, параграф 2, който изисква националните органи за защита на данните да издадат разрешение за трансферите на данни.

228 Директива за защита на личните данни, член 26, параграф 1, буква г).

229 Вж. по-специално Работна група за защита на личните данни по член 29 (2005 г.), *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995 [Работен документ за общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г.]*, WP 114, Брюксел, 25 ноември 2005 г.

6.4. Ограничено движение на данни към трети държави

Ключови въпроси

- Преди да изнася данни към трети държави, които не гарантират адекватно ниво на защита на данните, от администратора може да бъде изисканода подлага предвидените операции по предоставяне на дани на проверка от надзорния орган.
- По време на тази проверка администраторът, който желае да изнася данни, трябва да докаже две неща:
  - че е налице правно основание за трансфера на данни към получателя; и
  - че са налице мерки, които да гарантират адекватна защита на данните при получателя.
- Мерките за въвеждане на адекватна защита на данните при получателя могат да включват:
  - договорни клаузи между администратора, който изнася данни, и чуждестранния получател на данни; или
  - задължителни корпоративни правила, които обикновено са приложими спрямо трансферите на данни в рамките на международна група от дружества.
- Трансферите на данни към чуждестранни органи също могат да бъдат регулирани от специално международно споразумение.

Директивата за защита на личните данни и Допълнителният протокол към Конвенция № 108 позволяват на националното законодателство да установи режими за трансгранично предоставяне на данни към трети държави, които не гарантират ниво на защита на данните, дотолкова доколкото администраторът е сключил специални споразумения за осигуряване на адекватни гаранции за защита на данните при получателя, и докато администраторът може да докаже това пред компетентен орган. Това изискване е изрично посочено само в Допълнителния протокол към Конвенция № 108; при все това то се счита също така за стандартна процедура съгласно Директивата за защита на личните данни.

6.4.1. Договорни клаузи

Както в **правото на Съвета на Европа,** така и в **правото на ЕС,** като възможно средство за гарантиране на достатъчно ниво на защита на данните при получателя се посочват договорни клаузи между администратора, който изнася данни, и получателя в третата държава.

На **равнището на ЕС** Европейската комисия с помощта на Работната група по член 29 разработи стандартни договорни клаузи, които бяха официално признати като доказателство за адекватна защита на данните с решение на Комисията[230]. Тъй като решенията на Комисията са обвързващи, в своята цялост, за държавите членки, националните органи, които отговарят за контрола върху трансграничното предоставяне наданни, трябва да приемат тези стандартни договорни клаузи в своите процедури[231]. Така, ако администраторът, който изнася данни, и получателят от трета държава се споразумеят и подпишат тези клаузи, това би трябвало да предостави на надзорния орган достатъчно доказателства за наличието на адекватни гаранции.

Наличието на стандартни договорни клаузи в правната рамка на ЕС не забранява на администраторите да формулират други *ad hoc* договорни клаузи. Въпреки това, те би трябвало да осигуряват същото ниво на защита като предвиденото от стандартните договорни клаузи. Най-важните характеристики на стандартните договорни клаузи са:

- клауза в полза на трета страна, която дава възможност на физическите лица да упражняват договорни права дори ако те не са страна по договор;

- съгласието на получателя или вносителя на данни в случай на възникване на спор, той да се подчинява на процедурата на националния надзорен орган и/или съдилищата с юрисдикция на територията, на която се намира администраторът, който изнася данни.

Понастоящем съществуват две групи от стандартни клаузи за трансфери между администратори, между които администраторът, който изнася данни,

230 Директива за защита на личните данни, член 26, параграф 4.

231 ДФЕС, член 288.

може да избира[232]. Налице е само една група от стандартни договорни клаузи за трансфери между администратор и обработващ[233].

В контекста на **правото на Съвета на Европа** — Консултативният комитет към Конвенция № 108 състави ръководство за изготвянето на договорни клаузи[234].

6.4.2. Задължителни корпоративни правила

Многостранните задължителни корпоративни правила (ЗКП) много често включват едновременно няколко европейски органа за защита на данните[235]. За да бъдат одобрени, проектите на ЗКП трябва да бъдат изпратени на водещия орган заедно със стандартизираните формуляри[236]. Водещият орган може да се определи от стандартизираните формуляри за искане на одобрение. След това, този орган информира всички надзорни органи в държавите членки на ЕИП, в които са установени съдружници от групата, въпреки че участието им в процеса на оценка на ЗКП е доброволно. Въпреки че не е задължително, всички засегнати органи за защита на данните следва да включат резултата от оценката в своите редовни процедури за издаване на разрешение.

232 Набор I се съдържа в приложението към Решение 2001/497/ЕО на Комисията от 15 юни 2001 г. относно общите договорни клаузи за трансфера на лични данни към трети страни съгласно Директива 95/46/ЕО, ОВ L 181, 4.7.2001 г., Европейска комисия (2010 г.); Набор II се съдържа в приложението към Решение 2004/915/ЕО на Комисията от 27 декември 2004 г. за изменение на Решение 2001/497/ЕО за въвеждане на алтернативен комплект общи договорни клаузи за прехвърляне на лични данни в трети страни, ОВ L 385, 29.12.2004 г., Европейска комисия (2004 г.).

233 Европейска комисия (2010 г.), Решение 2010/87/ЕС на Комисията от 5 февруари 2010 г. относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета, ОВ L 39, 12.2.2010 г.

234 Съвет на Европа, Консултативен комитет към Конвенция № 108 (2002 г.), *Ръководство за изготвянето на договорни клаузи, които уреждат защитата на данни при трансфера на лични данни към трети лица, които нямат адекватно ниво на защита на данните*.

235 Съдържанието и структурата на подходящите задължителни корпоративни правила са обяснени от Работна група за защита на личните данни по член 29 (2008 г.), *Working document setting up a framework for the structure of Binding Corporate Rules [Работен документ за създаване на рамка за структурата на задължителните корпоративни правила]*, WP 154, Брюксел, 24 юни 2008 г., както и в Работна група за защита на личните данни по член 29 (2008 г.), *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules [Работен документ за създаване на таблица с елементите и принципите, които трябва да присъстват в задължителните корпоративни правила]*, WP 153, Брюксел, 24 юни 2008 г.

236 Работна група за защита на личните данни по член 29, *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data [Препоръка 1/2007 относно стандартното заявление за одобрение на задължителни корпоративни правила за трансфера на лични данни]*, WP 133, Брюксел, 10 януари 2007 г.

6.4.3. Специални международни споразумения

ЕС е сключил специални споразумения за предаване на два вида данни:

Резервационни данни на пътниците

Резервационните данни на пътниците (PNR) се събират от въздушните превозвачи при извършването на резервация и включват имената, адресите, подробности за кредитни карти и номерата на местата на пътниците във въздушния транспорт. Съгласно законодателството на САЩ въздухоплавателните дружества са длъжни да предоставят тези данни на Министерството на вътрешната сигурност преди заминаването на пътниците. Това се прилага по отношение на полети до и от САЩ.

За да се осигури адекватна защита на данните на пътниците в съответствие с разпоредбите на Директива 95/46/ЕО през 2004 г., беше приет набор от правила, свързани резервационни данни на пътниците[237]. Тези правила включват адекватността на обработката на данни, извършвана от Министерството по вътрешна сигурност (МВС) на САЩ.

В резултат на отмяната от СЕС на набора от правила, свързани с резервационните данни на пътниците[238], ЕС и САЩ подписаха две отделни споразумения с двойна цел. Първо, да се осигури правно основание за разкриването на резервационните данни на органите на САЩ; и второ, да се гарантираадекватна защита на данните в държавата получател.

Първото споразумение за начините, по които се обменят и управляват данните между държавите от ЕС и САЩ, подписано през 2012 г., имаше редица пропуски и беше заменено с ново споразумение от същата година с цел да се гарантира

237 Решение на Съвета 2004/496/ЕО от 17 май 2004 г. за сключване на Споразумение между Европийската общност и Съединените американски щати относно обработката и трансфера на резервационни данни на пътниците от въздухоплавателни дружества на Министерството на вътрешната сигурност на САЩ, Бюрото за митнически въпроси и гранична защита, ОВ 2004 L 183, стр.83 и Решение на Комисията 2004/535/ЕО от 14 май 2004 г. относно адекватната защита на личните данни, съдържащи се в резеврационните данни на пътниците, които се предоставят на американското Бюро за митнически въпроси и гранична защита, В 2004 L 235, стр. 11–22.

238 Съд на ЕС, Съединени дела, C-317/04 и C-318/04, *Европейски парламент с/у Съвета на Европейския съюз,* 30 май 2006 г., парагр. 57, 58 и 59, в които Съда отсъди, че решението за адекватност и споразумението, свързани с обработването на данни не влизат в обхвата на Директивата.

по-добра правната сигурност[239]. Новото споразумение предлага значителни подобрения. То ограничава и изяснява целите, за които може да се използва информацията, като например тежки международни престъпления и тероризъм и определя периода, през който данните могат да бъдат задържани: след шест месеца, данните трябва да бъдат деперсонализирани и маскирани В случай на злоупотреба с данните всекиима право на административна и съдебна защита. Те имат право също така на достъп до своите резервационни данни и да искат коригиране от Министерството на вътрешната сигурност, включително възможността за изтриване, ако информацията е неточна.

Споразумението, което влезе в сила на 1 юли 2012 г., ще действа за срок от седем години до 2019 г.

През декември 2011 г. Съветът на Европейския съюз одобри сключването на актуализирано Споразумение между Европейския съюз и Австралия относно обработката и предаването на резервационни данни за пътниците (PNR)[240]. Споразумението между ЕС и Австралия относно резервационните данни на пътниците (PNR) е още една стъпка в програмата на ЕС, която включва изготвянето на глобални насоки относно резервационните данни на пътниците[241], установяването на схема на ЕС за резервационни данни на пътниците[242] и воденето на преговори за споразумения с трети държави[243].

239 Решение 2012/472/ЕС на Съвета от 26 април 2012 г. за сключване на Споразумението между Съединените американски щати и Европейския съюз относно използването и предаването на резервационни данни на пътниците на Министерството на вътрешната сигурност на Съединените щати, ОВ L 215, 11.8.2012 г., стр. 4–4. Текстът на споразумението е приложен към решението, ОВ L 215, 11.8.2012 г., стр. 5–14.

240 Решение 2012/381/ЕС на Съвета от 13 декември 2011 г. за сключване на Споразумението между Европейския съюз и Австралия относно обработката и предаването на резервационни данни за пътниците (PNR) от въздушни превозвачи на Австралийската митническа и гранична служба, ОВ L 186, 14.7.2012 г., стр. 3–3. Текстът на споразумението, който замества предишното споразумение от 2008 г. е приложен към решението, ОВ L 186, 14.7.2012 г., стр. 4–16.

241 Вж. по-специално Съобщението на Комисията от 21 септември 2010 г. относно глобалния подход за предаване на резервационни данни на пътниците (PNR данни) на трети държави, COM(2010) 492 окончателен, Брюксел, 21 септември 2010 г. Също виж Работна група по член 29 (2010 г.), *Становище 7/2010 относно Съобщението на Европейската комисия относно глобалния подход за предаване на резервационни данни на пътниците (PNR данни) на трети държави,* РД 178, гр. Брюксел, 12 ноември 2010 г.

242 Предложение за директива на Европейския парламент и на Съвета относно използването на резервационни данни на пътниците за предотвратяване, разкриване, разследване и наказателно преследване на престъпления, свързани с тероризъм, и на тежки престъпления, COM(2011) 32 окончателен, Брюксел, 2 февруари 2011 г. През април 2011 г. Европейският парламент поиска FRA да даде становище относно това предложение и неговото съответствие с Хартата на основните права на Европейския съюз. Вж.: FRA (2011 г.), *Opinion 1/2011 – Passenger Name Record [Становище 1/2011 — Резервационни данни на пътниците (PNR)]*, Виена, 14 юни 2011 г.

243 ЕС води преговори за ново споразумение с Канада относно резервационните данни на пътниците, което ще замени действащото в момента споразумение от 2006 г.

Изпращане на финансови данни

Установеното в Белгия „Дружество за световни междубанкови финансови телекомуникации" (SWIFT), което обработва по-голямата част от световните парични преводи от европейски банки, извършва операции в подобни центове САЩ и му е било предявено искане да разкрие данни на Министерството на финансите на САЩ за целите на разследването на тероризма[244].

От гледната точка на ЕС нямаше налице достатъчно правно основание за разкриването на тези по същество европейски данни, които са били достъпни в САЩ само поради факта, че местонахождението на един от центровете на SWIFT за обработване на данни, свързани с услугата, е бил установен в САЩ.

През 2010 г. между ЕС и САЩ беше сключено специално споразумение, известно като Споразумението относно SWIFT, което да предостави необходимото правно основание и да гарантира достатъчна защита на данните[245].

Съгласно това споразумение финансовите данни, съхранявани от SWIFT, продължават да се предоставят на Министерството на финансите на САЩ за целите на предотвратяването, разследването, разкриването или наказателното преследване на тероризма или финансирането на тероризма. Министерството на финансите на САЩ може да изисква финансови данни от SWIFT, при условие че искането:

- посочва по възможно най-ясен начин финансовите данни;
- ясно обосновава необходимостта от данните;

244 Вж. в този контекст Работна група за защита на личните данни по член 29 (2011 г.), *Становище 14/2011 по въпроси за защита на личните данни, свързани с предотвратяването на изпирането на пари и финансирането на тероризма*, WP 186, Брюксел, 13 юни 2011 г.; Работна група за защита на личните данни по член 29 (2006 г.), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)* [*Становище 10/2006 относно обработката на лични данни от Дружеството за световна междубанкова финансова телекомуникация (SWIFT)*], WP 128, Брюксел, 22 ноември 2006 г.; Комисията на Белгия за защита на неприкосновеността на личния живот (*Commission de la protection de la vie privée*) (2008), *'Control and recommendation procedure initiated with respect to the company SWIFT scrl'[„Процедура за контрол и препоръки, започната по отношение на дружество SWIFT scrl"]*, Решение, 9 декември 2008 г.

245 Решение 2010/412/ЕС на Съвета от 13 юли 2010 г. относно сключването на Споразумението между Европейския съюз и Съединените американски щати относно обработката и изпращането на данни за финансови съобщения от Европейския съюз до Съединените щати за целите на Програмата за проследяване на финансирането на тероризма, ОВ L 195, 27.7.2010 г., стр. 3–4. Текстът на споразумението е приложен към решението, ОВ L 195, 2010 г., стр. 5–14.

- е формулирано възможно най-тясно, за да се сведе до минимум обемът на исканите данни;

- не се отнася за данни, свързани с Единната европейска платежна зона (SEPA).

Европол трябва да получи копие от всяко искане на Министерството на финансите на САЩ и да провери дали то съответства на принципите на Споразумението SWIFT[246]. Ако се потвърди съответствието на искането, SWIFT трябва да предостави финансовите данни непосредствено на Финансовото министерство на САЩ. Министерството трябва да съхранява финансовите данни в защитена физическа среда, където те са достъпни само за специалисти в разследването на терористични дейности или тяхното финансиране, като финансовите данни не трябва да бъдат свързани с никаква друга база данни. По принцип финансовите данни, получени от SWIFT, се заличават не по-късно от пет години след получаването им. Тезиданни, които са от значение за конкретни разследвания или наказателни преследвания, могат да се съхраняват за период, не по-дълъг от необходимото за тези разследвания или преследвания.

Министерството на финансите на САЩ може да предава информация от данните, получени от SWIFT, на конкретни правоприлагащи органи, органи за обществена сигурност или органи за борба с тероризма в рамите на САЩ или извън тях единствено за разследването, разкриването, предотвратяването или наказателното преследване на тероризма или неговото финансиране. Когато последващото предаване на финансови данни засяга гражданин на държава членка или лице, пребиваващо на територията на държава членка, всяко споделяне на данни с органи на трета държава е възможно само с предварителното съгласие на компетентните органи на засегната държава членка. Изключение може да се направи, когато споделянето на данни е от съществено значение за предотвратяването на непосредствена и сериозна заплаха за обществената сигурност.

Независими наблюдатели, включващи и лице, посочено от Европейската комисия, осъществяват мониторинг на спазването на принципите на Споразумението SWIFT.

246 Съвместният надзорен орган по Европол е извършил одити на дейностите в тази област, резулататите от които са налични на: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

Лицата, чиито данни се обработват, имат право да получат потвърждение от компетентния орган на ЕС за защита на данните, че техните права по отношение на защитата на личните данни са спазени. Съгласно Споразумението SWIFT, лицата, чиито данни се обработват, имат право също така на коригиране, изтриване или блокиране на данните, които са събрани и съхранявани за тях от Министерството на финансите на САЩ. Въпреки това обаче правата на достъп на лицата, чиито данни се обработват, може да подлежат на определени правни ограничения. При отказан достъп лицето, чиито данни се обработват, трябва да бъде информирано в писмена форма за отказа и за правото му да потърси административна и съдебна защита в САЩ.

Споразумението SWIFT е в сила за срок от пет години, до август 2015 г. Този срок се удължава автоматично за последващи срокове от една година освен ако някоя от страните уведоми другата най-малко шест месеца предварително за своето намерение да не продължава действието на споразумението.

7

Защитата на данните в контекста на полицията и наказателното правосъдие

ЕС	Обхванати въпроси	Съвет на Европа
	Общо по въпросите	Конвенция № 108
	Полиция	Препоръка за сектора на полицията
		ЕСПЧ, Решение от 17 декември 2009 г. по дело *B.B./Франция*, № 5335/06
		ЕСПЧ, Решение от 4 декември 2008 г. по дело *S. и Marper/Обединеното кралство*, № 30562/04 и 30566/04
		ЕСПЧ, Решение от 31 май 2005 г. по дело *Vetter/Франция*, № 59842/00
	Киберпрестъпност	Конвенция за престъпления в кибернетичното пространство
Защита на данните в контекста на трансграничното сътрудничество на полицейски и съдебни органи		
Рамково решение за защита на данните	**Общо по въпросите**	Конвенция № 108
		Препоръка за сектора на полицията
Решението от Прюм	**За специални данни: дактилоскопични отпечатъци, ДНК данни, хулиганство и т.н.**	Конвенция № 108
		Препоръка за сектора на полицията
Решението за ЕВРОПОЛ	**Чрез специални агенции**	Конвенция № 108
Решението за ЕВРОЮСТ		Препоръка относно използването на данни в сектора на полицията
Решението за Frontex		

Решението за Шенген II Регламентът за ВИС Регламентът за Евродак Решението за МИС	**Чрез специални съвместни информационни системи**	Конвенция № 108 Препоръка за сектора на полицията ЕСПЧ, Решение от 2 февруари 2010 г. по дело *Dalea/Франция*, № 964/07

За да се балансират интересите на физическите лица в областта на защитата на данните и интересите на обществото присъбирането на данни за целите на борбата с престъпността и гарантирането на националната и обществената сигурност, Съветът на Европа и ЕС са приели специални правни инструменти.

7.1. Право на Съвета на Европа относно защитата на данните във връзка с полицейски и наказателноправни въпроси

Ключови въпроси

- Конвенция № 108 и Препоръка на Съвета на Европа за сектора на полицията обхващат защитата на данните във всички области на полицейската работа.
- Конвенцията за престъпления в кибернетичното пространство *(Конвенция от Будапеща)* е задължителен международен правен инструмент, в който са обхванати престъпленията, извършени срещу и посредством електронни мрежи.

На европейско равнище Конвенция № 108 обхваща всички сфери на обработването на лични данни, като нейните разпоредби имат за цел да регламентират обработването на лични данни по принцип. Следователно Конвенция № 108 се прилага по отношение на защитата на данните в областта на полицията и наказателното правосъдие, макар че договарящите се страни могат да ограничат нейното приложение.

Установените от закона задачи на органите на полицията и наказателното правосъдие често налагат обработването на лични данни, което може да е свързано със сериозни последици за засегнатите физически лица. Препоръката за сектора на полицията, приета от Съвета на Европа през 1987 г., дава насоки на договарящите се страни относно начина, по който те следва да

приложат в действие принципите на Конвенция № 108 в контекста на обработването на лични данни от полицейските органи[247].

7.1.1. Препоръката за сектора на полицията

ЕСПЧ е последователен, като е постановявал, че съхраняването и запазването на лични данни от органите на полицията или на националната сигурност представлява намеса в правата по член 8, параграф 1 от ЕКПЧ. В много решения на ЕСПЧ се разглежда обосноваването на подобни случаи на намеса[248].

Пример: По делото *B.B./Франция*[249] ЕСПЧ реши, че включването на осъден извършител на сексуално престъпление в националната съдебна база данни попада в обхвата на член 8 от ЕКПЧ. Въпрекитова,предвид факта, че са били приложени достатъчно предпазни мерки за защита на данните, като правото на съответното физическо лице да поиска изтриването на данните, ограниченото времетраене на тяхното съхранение и ограничения достъп до тях, е бил намерен справедлив баланс между заложените противоречащи си частни и обществени интереси. Съдът е заключил, че не е налице нарушение на член 8 от ЕКПЧ.

Пример: По делото *S. и Marper/Обединеното кралство*[250] и двамата жалбоподатели са били обвинени в извършването на престъпление, но не са били осъдени. Независимо от това техните дактилоскопични отпечатъци, проби от ДНК профили и клетки се пазят и съхраняват от полицията. Неограниченото запазване на биометрични данни е било позволено от закона, ако лицето е било заподозряно в извършването на престъпление, дори ако по-късно заподозреният е намерен за невинен или е бил оправдан. ЕСПЧ постанови, че повсеместното и неизбирателно запазване на лични данни без ограничение на периода от време и ограничените възможности на да поискат заличаване, представлява непропорционална

247 Съвет на Европа, Комитет на министрите (1987 г.), Препоръка Rec(87)15 до държавите членки за уреждане на използването на лични данни в сектора на полицията, 17 септември 1987 г.

248 Вж. например ЕСПЧ, Решение от 26 март 1987 г. по дело *Leander/Швеция*, № 9248/81; ЕСПЧ, Решение от 13 ноември 2012 г. по дело *M.M./Обединеното кралство*, № 24029/07; ЕСПЧ, Решение от 18 април 2013 г. по дело *M.K./Франция*, № 19522/09.

249 ЕСПЧ, Решение от 17 декември 2009 г. по дело *B.B./Франция*, № 5335/06.

250 ЕСПЧ, Решение от 4 декември 2008 г. по дело *S. и Marper/Обединеното кралство*, № 30562/04 и 30566/04, точки 119 и 125.

намеса в правото на зачитане на личния живот на жалбоподателите. Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

В много последващи решения на ЕСПЧ се разглежда обосноваването на намесата в правото на защита на данните при полицейско наблюдение.

Пример: По делото *Allan/Обединеното кралство*[251] частните разговори на затворник с приятел в зоната за посетители в затвора и със съобвинен в затворническата килия са били записани тайно от органите. ЕСПЧ постанови, че използването на устройства за аудио- и видеозапис в килията на жалбоподателя, в зоната за посетители в затвора и носени от съзатворник означават намеса в правото на неприкосновеност на личния живот на жалбоподателя. Тъй като не е била налице правноустановена система, регламентираща използването на скрити записващи устройства от полицията в съответния момент, посочената намеса не е била в съответствие със закона. Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

Пример: По делото *Klass и други/Германия*[252] жалбоподателите твърдят, че няколко германски законодателни акта, позволяващи тайно наблюдение на електронната поща, кореспонденцията и далекосъобщенията, са нарушили член 8 от ЕКПЧ, по-специално поради факта, че засегнатото лице не е било информирано относно мерките за наблюдение и не е могло да отнесе въпроса до съда, когато мерките са били прекратени. ЕСПЧ е постановил, че опасността от наблюдение неминуемо представлява намеса в свободата на комуникация между потребителите на пощенски и далекосъобщителни услуги. Въпреки това Съдът обаче е установил, че са били приложени достатъчни предпазни мерки срещу злоупотреба. Потвърди се правотата на германския законодателен орган, който е счел подобни мерки за необходими в демократично общество в интерес на националната сигурност и за предотвратяването на безредие или извършване на престъпление. Съдът е заключил, че не е налице нарушение на член 8 от ЕКПЧ.

Тъй като обработването на данни от полицейските органи може да има значително въздействие върху засегнатите лица, подробни правила относно защитата на данните са особено необходими за поддържането на бази данни в

251 ЕСПЧ, Решение от 5 ноември 2002 г. по дело *Allan/Обединеното кралство*, № 48539/99.

252 Решение от 6 септември 1978 г. по дело *Klass и други/Германия*, № 5029/71.

тази област. Стремежът в препоръката на Съвета на Европа за сектора на полицията е да бъде разгледан въпросът чрез предоставянето на насоки относно начините, по които следва да се събират данните за полицейска работа; как следва да се съхраняват досиетата в тази област; кой следва да има разрешение за достъп до досиетата, включително условията за предаване на данни на чуждестранни полицейски органи; как съответните физически лица да могат да упражняват своите права на защита на данните; как да се упражнява контрол от независимите органи. Взето е под внимание и задължението за осигуряване на подходяща сигурност на данните.

Препоръката не предвижда неограничено неизбирателно събиране на данни от полицейските органи. Тя ограничава събирането на лични данни от полицейските органи до необходимото за предотвратяването на реална опасност или възпирането на конкретно престъпление. Събиране на всякакви допълнителни данни би трябвало да се основава на специално национално законодателство. Обработването на чувствителни данни следва да бъде ограничено до това, което е абсолютно необходимо в контекста на конкретно проучване.

Ако личните данни се събират без знанието на съответните физически лица, те трябва да бъдат информирани за събирането на данните веднага, когатоподобно разкриване вече не възпрепятства разследванията. Събирането на данни със средства за техническо наблюдение или други автоматизирани средства също следва да се основава на специални правни разпоредби.

Пример: По делото *Vetter/Франция*[253] жалбоподателят е бил обвинен в убийство от анонимен свидетел. Тъй като жалбоподателят редовно ходел в дома на приятел, полицията инсталирала подслушвателни устройства там с разрешението на разследващия съдия. Въз основа на записаните разговори жалбоподателят бил арестуван и изправен пред съда за убийство. Той подал молба записите да бъдат обявени за недопустими като доказателство, като по-специално привел довода, че това не било предвидено от закона. За ЕСПЧ спорният въпрос е бил дали използването на подслушвателни устройства е било „в съответствие със закона“. Инсталирането на микрофони за подслушване в частни помещения очевидно не попадало в обхвата на член 100 *и следв.* от Наказателнопроцесуалния кодекс, тъй като тези разпоредби се отнасяли до прихващането на

253 ЕСПЧ, Решение от 31 май 2005 г. по дело *Vetter/Франция*, № 59842/00.

комуникации по телефонни линии. В член 81 от кодекса не се е посочвал достатъчно ясно обхвата или начина на упражняване на правото на преценка на органите при разрешаването на прослушването на частни разговори. Следователно жалбоподателят не се е ползвал от минималната степен на защита, на която имат право гражданите в съответствие с принципа за върховенство на закона в демократичното общество. Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

В препоръката се заключава, че когато се съхраняват лични данни, следва да се направят ясни разграничения между: административни и полицейски данни; различните видове физически лица, например заподозрени, осъдени лица, жертви и свидетели; данни, считани за установени факти, и такива, основаващи се на подозрения или предположение.

Полицейските данни следва да бъдат строго ограничени по отношение на целта. Това има последици за съобщаването на полицейски данни на трети страни: трансферът или съобщаването на такива данни в рамките на сектора на полицията следва да се ръководи от това дали е налице законен интерес от обмена на информацията. Трансферът или съобщаването на такива данни извън сектора на полицията следва да се допуска само ако е налице ясно правно задължение или разрешение. Международният трансфер или съобщаване трябва да се ограничават до чуждестранни полицейски органи и да се основават на специални правни разпоредби, по възможност международни споразумения, освен ако не са необходими за предотвратяването на сериозна, и непосредствена опасност.

Обработването на данни от полицията трябва да подлежи на независим надзор, за да се гарантира съответствието с националното законодателство за защита на данните. Физическите лица, чиито данни се обработват, трябва да имат всички права за достъп до данните, включени в Конвенция № 108. Ако правата за достъп на лицата, чиито данни се обработват, са ограничени в съответствие с член 9 от Конвенция № 108 в интерес на провеждането на ефективни полицейски разследвания, те трябва да имат право съгласно националното законодателство да подадат жалба до националния надзорен орган за защита на данните или до друг независим орган.

7.1.2. Конвенцията от Будапеща за престъпленията в кибернетичното пространство

Престъпната дейност все повече използва и засяга електронни системи за обработване на данни, поради което са необходими нови наказателноправни разпоредби за справяне с това предизвикателство. По тази причина Съветът на Европа прие международен правен инструмент — Конвенция за престъпленията в кибернетичното пространство, известна също като Конвенцията от Будапеща, за разглеждане на въпроса за престъпленията, извършени срещу и с помощта на електронни мрежи[254]. Конвенцията е отворена за присъединяване и на държави, които не са членки на Съвета на Европа, като до средата на 2013 г. четири държави извън Съвета на Европа — Австралия, Доминиканската република, Япония и САЩ — станаха страни по конвенцията, а още 12 други държави, които не са членки, са я подписали или са били поканени да се присъединят към нея.

Конвенцията за престъпленията в кибернетичното пространство остава най-влиятелният международен договор, разглеждащ нарушенията на законодателството в интернет или други информационни мрежи. Тя изисква от страните по нея да актуализират и хармонизират своите наказателни закони срещу компютърното пиратство и други нарушения на сигурността, включващи нарушения на авторското право, компютърните измами, детската порнография и други незаконни дейности в кибернетичното пространство. Конвенцията предвижда също така процесуални правомощия, обхващащи претърсването на компютърни мрежи и прихващането на съобщения в контекста на борбата с престъпленията в кибернетичното пространство. Накрая, тя позволява ефективното международно сътрудничество. В Допълнителен протокол към конвенцията се разглежда инкриминирането на расистка и ксенофобска пропаганда в компютърните мрежи.

В действителност конвенцията не е инструмент за насърчаване на защитата на данните, но тя инкриминира дейности, които е възможно да нарушат правото на съответното физическо лице на защита на неговите данни. Тя също така задължава договарящите се страни, когато прилагат конвенцията, да предвидят адекватна защита на правата и свободите на човека, включително правата, гарантирани от ЕКПЧ, например правото на защита на данните[255].

254 Съвет на Европа, Комитет на министрите (2001 г.), Конвенция за престъпления в кибернетичното пространство, CETS № 185, Будапеща, 23 ноември 2001 г., влязла в сила на 1 юли 2004 г.

255 *Пак там*, член 15, параграф 1.

7.2. Право на ЕС в областта на защитата на данните във връзка с полицейски и наказателноправни въпроси

Ключови въпроси

- На равнището на ЕС защитата на данни в сектора на полицията и наказателното правосъдие е уредена само в контекста на трансграничното сътрудничество на полицейски и съдебни органи.
- Специални режими за защита на данните съществуват за Европейската полицейска служба (ЕВРОПОЛ) и Европейското звено за съдебно сътрудничество (ЕВРОЮСТ), които са органи на ЕС, подпомагащи и насърчаващи трансграничното правоприлагане.
- Специални режими за защита на данните съществуват и за съвместните информационни системи, установени на равнището на ЕС за трансграничен обмен на информация между компетентните полицейски и съдебни органи. Важни примери са Шенген II, Визовата информационна система (ВИС) и Евродак — централизирана система, съдържаща дактилоскопични данни на граждани на трети държави, кандидатстващи за убежище в една от държавите членки на ЕС.

Директивата за защита на данните не се прилага в областта на полицията и наказателното правосъдие. В раздел 7.2.1 са описани най-важните правни инструменти в тази област.

7.2.1. Рамковото решение за защита на данните

Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси *(Рамковото решение за защита на данните)*[256] има за цел предоставянето на защита за личните данни на физическите лица, когато тези данни се обработват за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпление или изпълнението на наказателна санкция. От името на държавите членки или на ЕС действат компетентни органи,

256 Съвет на Европейския съюз (2008 г.), Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси (*Рамково решение за защита на данните*), ОВ L 350, 30.12.2008 г.

работещи в сферата на полицията и наказателното правосъдие. Тези органи са агенции или органи на ЕС, както и органите на държавите членки[257]. Приложимостта на рамковото решение е ограничена до осигуряването на защита на данните при трансграничното сътрудничество между тези органи и не обхваща националната сигурност.

Рамковото решение за защита на данните се основава в голяма степен на принципите и определенията, които се съдържат в Конвенция № 108 и в Директивата за защита на личните данни.

Данните трябва да се използват само от дадения компетентен орган и само за целта, за която са били изпратени или предоставени. Получаващата държава членка трябва да спазва всички ограничения относно обмена на данни, предвидени в законодателството на изпращащата държава членка. Използването на данни от държавата получател за друга цел обаче е разрешено при определени условия. Регистрирането и документирането на предаването на данни е специално задължение на компетентните органи, за да съдействат за изясняване на отговорностите, произтичащи от жалбите. За последващия трансфер на данни, получени в хода на трансграничното сътрудничество, към трети лица е необходимо съгласието на държавата членка, от която са получени данните, въпреки че за спешни случаи са предвидени изключения.

Компетентните органи трябва да вземат необходимите мерки за сигурност с цел защита на личните данни срещу всякакви незаконни форми на обработване.

Всяка държава членка трябва да гарантира, че един или повече независими национални надзорни органи отговарят за консултиране и мониторинг на прилагането на разпоредбите, приети съгласно Рамковото решение за защита на данните. Те също така разглеждат искове, подадени от което и да е лице, отнасящи се до защитата на неговите права и свободи във връзка с обработването на лични данни от страна на компетентните органи.

Съответното физическо лице има право на информация за обработването на неговите лични данни и има право на достъп, коригиране, изтриване или блокиране. Когато упражняването на тези права е отказано въз основа на първостепенни съображения, физическото лице трябва да има право да обжалва

257 *Пак там*, член 2, буква з).

пред компетентния национален надзорен орган и/или съд. Ако на дадено лице бъде причинена вреда поради нарушения на националното законодателство за прилагане на Рамковото решение за защита на данните, това лице има право на обезщетение от администратора[258]. По принцип физическите лица трябва да имат достъп до средство за правна защита в случай на нарушение на техните права, гарантирани от националното законодателство за прилагане на Рамковото решение за защита на данните[259].

Европейската комисия предложи реформа, която се състои от общ регламент относно защитата на данните[260] и директива за защита на данните[261]. Тази нова директива ще замени настоящото Рамково решение за защита на данните и ще въведе общи принципи и правила в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси.

7.2.2. По-специфични правни инструменти в областта на защитата на данните при трансгранично сътрудничество на полицейски и правоприлагащи органи

В допълнение към Рамковото решение за защита на данните обменът на информация, съхранявана от държавите членки в специфични области, се урежда от редица правни инструменти, като например Рамково решение 2009/315/ПВР на Съвета относно организацията и съдържанието на обмена на информация, получена от регистрите за съдимост, между държавите членки и Решение на Съвета относно условията за сътрудничество и

258 *Пак там*, член 19.

259 *Пак там*, член 20.

260 Европейска комисия (2012 г.), *Предложение за регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (общ регламент относно защитата на данните*), COM(2012)011 окончателен, Брюксел, 25 януари 2012 г.

261 Европейска комисия (2012 г.), *Предложение за директива на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни (обща директива за защита на личните данни)*, COM(2012)010 окончателен, Брюксел, 25 януари 2012 г.

обмен на информация между звената за финансово разузнаване на държавите членки[262].

Най-важното е, че трансграничното сътрудничество[263] между компетентните органи включва във все по-голяма степен обмена на имиграционни данни. Тази област от правото не касае полицията и наказателното правосъдие, но в много отношения тя е свързана с работата на полицията и правосъдните органи. Същото важи и за данните за стоките, които се внасят във или се изнасят от ЕС. Премахване на контрола по вътрешните граници в рамките на ЕС е увеличило риска от измами, което е наложило засилване на сътрудничеството между държавите членки, най-вече чрез увеличаване на трансграничния обмен на информация, за да може по-ефективно да се разкриват нарушения на националното и европейското митническо законодателство.

Решението от Прюм

Важен пример за институционализирано трансгранично сътрудничество чрез обмен на съхранявани на национално равнище данни е Решение 2008/615/ПВР на Съвета за засилване на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност (*Решението от Прюм*), с което Договорът от Прюм беше въведен в правото на ЕС през 2008 г.[264]. Договорът от Прюм беше международно споразумение за полицейско сътрудничество, подписано през 2005 г. от Австрия, Белгия, Франция, Германия, Люксембург, Нидерландия и Испания[265].

---

262 Съвет на Европейския съюз (2009 г.), Рамково решение 2009/315/ПВР на Съвета от 26 февруари 2009 г. относно организацията и съдържанието на обмена на информация, получена от регистрите за съдимост, между държавите членки, ОВ L 93, 7.4.2009 г.; Съвет на Европейския съюз (2000 г.), Решение на Съвета от 17 октомври 2000 г. относно условията за сътрудничество и обмен на информация между звената за финансово разузнаване на държавите членки, ОВ L 271, 24.10.2000 г.

263 Европейска комисия (2012 г.), Съобщение на Комисията до Европейския парламент и Съвета – Засилване на сътрудничеството в областта на правоприлагането в ЕС: Европейският модел за обмен на информация (EIXM), COM(2012) 735 окончателен, Брюксел, 7 декември 2012 г.

264 Съвет на Европейския съюз (2008 г.), Решение 2008/615/ПВР на Съвета от 23 юни 2008 г. за засилване на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност, ОВ L 210, 6.8.2008 г.

265 Договор между Кралство Белгия, Федерална република Германия, Кралство Испания, Френската република, Великото херцогство Люксембург, Кралство Нидерландия и Република Австрия относно засилване на презграничното сътрудничество, особено в борбата с тероризма, презграничната престъпност и нелегалната миграция, достъпен на адрес: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

Целта на решението от Прюм е да се помогне на държавите членки да подобрят обмена на информация за целите на предотвратяването и борбата с престъпността в три области: тероризма, трансграничната престъпност и незаконната миграция. За тази цел решението определя разпоредби по отношение на:

- автоматичния достъп до ДНК профили, дактилоскопични данни и определени данни от националната регистрация на превозните средства;
- предоставянето на данни, свързани с големи събития с трансгранично измерение;
- предоставянето на информация с цел предотвратяване на терористични престъпления;
- други мерки за засилване на трансграничното полицейско сътрудничество.

Базите данни, които са предоставени на разположение по силата на Решението от Прюм, се уреждат изцяло от националното законодателство, но обменът на данни допълнително се регламентира в решението, а отскоро — и в Рамковото решение за защита на данните. Компетентните органи за надзор на тези трансфери наданни са националните надзорни органи за защита на данните.

7.2.3. Защита на данните в рамките на ЕВРОПОЛ и ЕВРОЮСТ

ЕВРОПОЛ

ЕВРОПОЛ, агенцията на ЕС за правоприлагане, е със седалище в Хага и разполага с национални звена на ЕВРОПОЛ (НЗЕ) във всяка държава членка. ЕВРОПОЛ е създадена през 1998 г.; настоящият ѝ правен статут като институция на ЕС се основава на Решението на Съвета за създаване на Европейска полицейска служба (*Решението за ЕВРОПОЛ*)[266]. Целта на ЕВРОПОЛ е да

266 Съвет на Европейския съюз (2009 г.), Решение 2009/371/ПВР на Съвета от 6 април 2009 г. за създаване на Европейска полицейска служба (Европол), OB L 121, 15.5.2009 г. Вж. също с оглед на това предложението на Комисията за регламент, което предвижда правна рамка за създаване на нова Европол, която е правоприемник на Европол, създадена с Решение 2009/371/ПВР на Съвета от 6 април 2009 г. за създаване на Европейска полицейска служба (Европол), и правоприемник на Европейския полицейски колеж (CEPOL), създаден с Решение 2005/681/ПВР на Съвета за създаване на Европейски полицейски колеж (ЕПК), COM(2013) 173 окончателен.

съдейства за предотвратяването и разследването на организираната престъпност, тероризма и други тежки форми на престъпност, посочени в приложението към Решението за ЕВРОПОЛ, които засягат две или повече държави членки.

За да постигне своите цели, ЕВРОПОЛ е създала информационната система на ЕВРОПОЛ, която представлява база данни за обмен на разузнавателни данни и информация, свързани с престъпления, между държавите членки чрез техните НЗЕ. Информационната система на ЕВРОПОЛ може да се използва за предоставяне на данни, които се отнасят до: лица, които са заподозрени или които са били осъдени за извършването на престъпление, което попада в компетентността на ЕВРОПОЛ, или лица, за които са налице факти да се счита, че ще извършат такива престъпления. ЕВРОПОЛ и НЗЕ могат да въвеждат директно данни в информационната система на ЕВРОПОЛ и да извличат данни от нея. Единствено страната, която е въвела данните в системата, може да ги променя, коригира или заличава.

Когато е необходимо за изпълнението на задачите ѝ, ЕВРОПОЛ може да съхранява, изменя и използва в аналитичните работни досиета данни за престъпления. Аналитичните работни досиета се отварят за целите на събирането, обработването или използването на данните, за да се подпомогнат конкретни наказателни разследвания, водени от ЕВРОПОЛ съвместно с държави членки на ЕС.

В отговор на новите развития, на 1 януари 2013 г., в ЕВРОПОЛ беше създаден Европейски център по киберпрестъпност[267]. Центърът служи като централно европейско информационно звено по въпросите на киберпрестъпността, което допринася за по-бързи реакции в случай на онлайн престъпления, разработва и разгръща цифрови съдебно-технически възможности и предоставя добри практики от разследвания на престъпления в кибернетичното пространство. Центърът акцентира върху престъпления в кибернетичното пространство, които:

- са извършени от организирани престъпни групи с цел реализиране на големи печалби, като например онлайн измами;

267 Вж. също ЕНОЗД (2012 г.), *Становище на Европейския надзорен орган по защита на данните относно съобщението на Европейската комисия до Съвета и Европейския парламент за създаването на Европейски център по киберпрестъпност*, Брюксел, 29 юни 2012 г.

- причиняват тежки щети на жертвите, например сексуална експлоатация на деца онлайн;

- засягат ключова инфраструктура и информационни системи в ЕС.

Режимът за защита на данните, който урежда дейността на ЕВРОПОЛ, е засилен. Член 27 от Решението за ЕВРОПОЛ гласи, че по отношение на обработването на автоматизираните и неавтоматизираните данни се прилагат принципите, които са посочени в Конвенция № 108 и в Препоръката за сектора на полицията. При предаването на данни между ЕВРОПОЛ и държавите членки трябва да се спазват също така правилата, съдържащи се в Рамковото решение за защита на данните.

За да се гарантира съответствието с приложимото право в областта на защитата на данните и по-специално, че не се нарушават правата на лицата при обработването на личните данни, независимият съвместен надзорен орган (СНО) на ЕВРОПОЛ извършва преглед и контрол върху дейностите на ЕВРОПОЛ[268]. Всяко физическо лице има право на достъп до всички лични данни, които ЕВРОПОЛ може да съхранява за него, в допълнение към правото да поиска тези лични данни да бъдат проверени, коригирани или изтрити. Ако дадено лице не е удовлетворено от решението на ЕВРОПОЛ относно упражняването на тези права, то може да подаде жалба до Комисията по жалби на СНО.

Ако настъпят щети в резултат на правни или фактически грешки в данните, съхранявани или обработвани в ЕВРОПОЛ, засегнатото физическо лице може да търси защита само пред компетентния съд на държавата члена, в която е възникнало, предизвикалото щета, събитие[269]. ЕВРОПОЛ възстановява заплатените като обезщетение суми, ако щетите са в резултат на неспазване на неговите правни задължения.

ЕВРОЮСТ

ЕВРОЮСТ е създадено през 2002 г. като орган на ЕС с централен офис в Хага, който насърчава съдебното сътрудничество в разследванията и

268 Решение за ЕВРОПОЛ, член 34.

269 *Пак там*, член 52.

наказателните преследвания относно тежкатапрестъпност, която засяга поне две държави членки[270]. ЕВРОЮСТ има компетенции:

- да насърчава и подобрява координацията на разследванията и наказателните преследвания между компетентните органи на отделните държави членки;

- да улеснява изпълнението на искания и решения, отнасящи се до съдебното сътрудничество.

Функциите на ЕВРОЮСТ се изпълняват от национални членове. Всяка държава членка изпраща съдия или прокурор в ЕВРОЮСТ, чийто статут се подчинява на националното право и който е овластен с необходимите правомощия, за да изпълнява необходимите задачи за насърчаване и подобряване на съдебното сътрудничество. Освен това, националните членове действат съвместно като колегиален орган за изпълнението на специалните задачи на ЕВРОЮСТ.

ЕВРОЮСТ може да обработва лични данни, доколкото това е необходимо за постигането на неговите цели. Това обаче е ограничено до точно определена информация относно лицата, които са заподозрени в извършване или участие в престъпление или са осъдени за престъпление, което попада в областта на компетентност на ЕВРОЮСТ. ЕВРОЮСТ може да обработва също така определена информация относно свидетели или жертви на престъпления, които попадат в областта на неговата компетентност[271]. В извънредни случаи, ЕВРОЮСТ може да обработва за ограничен период от време по-широк кръг от лични данни относно обстоятелствата, свързани с престъпление, когато такива данни имат непосредствено отношение към текущо разследване. В рамките на своята компетентност ЕВРОЮСТ може да си сътрудничи с други институции, органи и агенции на ЕС и да обменя лични данни с тях. ЕВРОЮСТ

270 Съвет на Европейския съюз (2002 г.), Решение 2002/187/ПВР на Съвета от 28 февруари 2002 г. за създаване на Евроюст с оглед засилване на борбата срещу сериозната престъпност, ОВ L 63, 6.3.2002 г.; Съвет на Европейския съюз (2003 г.), Решение 2003/659/ПВР на Съвета от 18 юни 2003 г. за изменение на Решение 2002/187/ПВР за създаване на Евроюст за засилване борбата срещу сериозната престъпност, ОВ L 44, 29.9.2003 г.; Съвет на Европейския съюз (2009 г.), Решение 2009/426/ПВР на Съвета от 16 декември 2008 г. за укрепване на Евроюст и за изменение на Решение 2002/187/ПВР за създаване на Евроюст с оглед засилване на борбата срещу сериозната престъпност, ОВ L 138, 4.6.2009 г. (*решенията относно ЕВРОЮСТ*).

271 Консолидиран текст на Решение 2002/187/ПВР на Съвета, изменено с Решение 2003/659/ПВР на Съвета и с Решение 2009/426/ПВР на Съвета, член 15, параграф 2.

може също така да си сътрудничи и да обменя лични данни с трети държави и организации.

По отношение на защитата на данните ЕВРОЮСТ трябва да гарантира ниво на защита поне еквивалентно на принципите на Конвенция № 108 на Съвета на Европа и нейните последващи изменения. В случаи на обмен на данни трябва да се спазват определени правила и ограничения, които се въвеждат или в споразумение за сътрудничество, или в работно споразумение в съответствие с решенията на Съвета относно ЕВРОЮСТ и неговия процедурен правилник[272].

Създаден е независим съвместен надзорен орган (СНО) със задача да наблюдава обработването на лични данни, осъществявано от ЕВРОЮСТ. Физическите лица могат да изпращат жалби до СНО, ако не са удовлетворени от отговора на ЕВРОЮСТ на искането им за достъп, коригиране, блокиране или изтриване на лични данни. Ако ЕВРОЮСТ обработва незаконно лични данни, подлежи на отговорност в съответствие с националното законодателство на държавата членка, където са разположени централните му офиси — Нидерландия, за всяка вреда, причинена на съответното физическо лице.

7.2.4. Защита на данните в рамките на съвместните информационни системи на равнището на ЕС

В допълнение към обмена на данни между държавите членки и създаването на специализирани органи на ЕС за борба с трансграничната престъпност са изградени няколко съвместни информационни системи на равнището на ЕС, които да служат като платформа за обмен на данни между компетентните национални органи и органи на ЕС за точно определени цели на правоприлагането, включително на правото в областта на миграцията и митническото право. Някои от тези системи се развиха вследствие на многостранни споразумения, които впоследствие бяха заменени от правни инструменти и системи на ЕС, като Шенгенската информационна система, Визовата информационна система, Евродак, Европейската система за наблюдение на границите (EUROSUR) или Митническата информационна система.

272 Процедурен правилник за обработване и защита на лични данни в Евроюст, ОВ C 68, 19.3.2005 г., стр. 1.

Европейската агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието (eu-LISA)[273], създадена през 2012 г., отговаря за дългосрочното оперативно управление на Шенгенска информационна система от второ поколение (ШИС II), Визовата информационна система (ВИС) и Евродак. Основната задача на eu-LISA е да осигурява ефективно, защитено и непрекъснато функциониране на информационните системи. Тя отговаря също така за приемането на необходимите мерки за гарантиране на сигурността на системите и сигурността на данните.

Шенгенската информационна система

През 1985 г. няколко държави членки от предишните Европейски общности се присъединиха към Споразумението между държавите от Икономическия съюз на Бенелюкс, Германия и Франция относно постепенната отмяна на проверките по общите граници (*Шенгенското споразумение*), което имаше за цел създаването на пространство за свободното движение на хора, невъзпрепятствано от гранични проверки в рамките на Шенгенската територия[274]. С цел неутрализиране на заплахата за обществената сигурност, която би могла да произтича от отворените граници, бяха въведени засилени гранични проверки по външните граници на Шенгенското пространство, както и тясно сътрудничество между националните полицейски и съдебни органи.

Като последица от присъединяването на още държави към Шенгенското споразумение, накрая, Шенгенската система беше включена в правната рамка на ЕС с Договора от Амстердам[275]. Това решение беше взето през 1999 г. Най-новата версия на Шенгенската информационна система, т. нар. ШИС II, започна да функционира на 9 април 2013 г. Сега тя служи на всички държави членки

273 Регламент (ЕС) № 1077/2011 на Европейския парламент и на Съвета от 25 октомври 2011 г. за създаване на Европейска агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието, ОВ L 286, 1.11.2011 г.

274 Споразумение между правителствата на държавите от Икономическия съюз на Бенелюкс, Федерална република Германия и Френската република за постепенното премахване на контрола по техните общи граници, ОВ L 239, 2000 г.

275 Европейски общности (1997 г.), Договор от Амстердам, изменящ Договора за Европейския съюз, Договорите за създаване на Европейските общности и някои свързани с тях актове, ОВ C 340, 10.11.1997 г.

на ЕС, Исландия, Лихтенщайн, Норвегия и Швейцария[276]. ЕВРОПОЛ и ЕВРОЮСТ също имат достъп до ШИС II.

ШИС II се състои от централна система (Ц-ШИС), национална система (Н-ШИС) във всяка държава членка и комуникационна инфраструктура между централната система и националните системи. Ц-ШИС съдържа определени данни относно лица и обекти, въвеждани от държавите членки. Ц-ШИС се използва от националните органи за граничен контрол, полицейските, митническите, визовите и съдебните органи в рамките на цялото Шенгенско пространство. Всяка държава членка управлява национално копие на Ц-ШИС, известно като национална Шенгенска информационна система (Н-ШИС), която се актуализира постоянно, като по този начин актуализира Ц-ШИС. Справки в Н-ШИС се правят и се подава сигнал, когато:

- лицето няма право да влиза или пребивава на Шенгенска територия;
- лицето или обектът се издирват от съдебни или правоприлагащи органи;
- лицето е обявено за изчезнало; или
- стоки, като например банкноти, автомобили, камиони, огнестрелно оръжие и документи за самоличност, са обявени за откраднати или изгубени.

При подаден сигнал трябва да започнат последващи действия чрез националната Шенгенска информационна система.

ШИС II има нови функции, като възможността за въвеждане на биометрични данни, например дактилоскопични отпечатъци и снимки, или на нови категории сигнали, като откраднати плавателни съдове, самолети, контейнери или платежни средства, както и по-разширени сигнали относно лица и обекти, копия на Европейски заповеди за арест по отношение на лица, издирвани за арест, предаване или екстрадиране.

276 Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. за създаването, функционирането и използването на Шенгенска информационна система от второ поколение *(ШИС II)*, ОВ L 381, 28.12.2006 г. и Съвет на Европейския съюз (2007 г.), Решение 2007/533/ПВР на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение *(ШИС II)*, ОВ L 205, 7.8.2007 г.

Решение 2007/533/ПВР на Съвета относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) (Решението за Шенген II) включва Конвенция № 108: „Личните данни, обработвани при прилагане на настоящото решение, са защитени в съответствие с Конвенцията на Съвета на Европа“ — Конвенция № 108[277]. Когато използването на лични данни от националните полицейски органи се извършва при прилагане на Решението за Шенген II, разпоредбите на Конвенция № 108, както и на Препоръката относно използването на данни в сектора на полицията, трябва да бъдат приложени в националното законодателство.

Компетентният национален надзорен орган във всяка държава членка осъществява надзор върху вътрешната Н-ШИС. По-специално, той трябва да провери качеството на данните, които държавата членка въвежда в Ц-ШИС посредством Н-ШИС. Националният надзорен орган трябва да гарантира, че най-малко веднъж на четири години се извършва одит на операциите по обработване на данни в рамките на вътрешната Н-ШИС. Националните надзорни органи и ЕНОЗД си сътрудничат и осигуряват координиран надзор на ШИС, докато ЕНОЗД отговоря за надзора на Ц-ШИС. С цел осигуряване на прозрачност на всеки две години се изпраща съвместен доклад за дейността на Европейския парламент, Съвета и eu-LISA.

Правата на достъп на лицата по отношение на ШИС II могат да се упражняват във всяка държава членка, тъй като всяка Н-ШИС е точно копие на Ц-ШИС.

Пример: По делото *Dalea/Франция*[278] жалбоподателят е получил отказ за виза за посещение във Франция, тъй като френските органи са съобщили в Шенгенската информационна система, че следва да му бъде отказано влизане. Жалбоподателят се е опитал безуспешно да получи достъп и коригиране или заличаване на данните пред френската Комисия за защита на данните, а накрая — пред Държавния съвет. ЕСПЧ е постановил, че съобщението за жалбоподателя в Шенгенската информационна система е било в съответствие със закона и е преследвало законната цел за защита на националната сигурност. Тъй като жалбоподателят не е доказал по какъв начин е бил наистина засегнат в резултат на отказа за

277 Съвет на Европейския съюз (2007 г.), Решение 2007/533/ПВР на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (*ШИС II*), ОВ L 205, 7.8.2007 г., член 57.

278 ЕСПЧ, Решение от 2 февруари 2010 г. по дело *Dalea/Франция* (dec.), № 964/07.

влизане в Шенгенското пространство и тъй като са били приложени достатъчно мерки, за да бъде защитен той от произволни решения, намесата в правото му на зачитане на личния живот е била пропорционална. Така жалбата по член 8 на жалбоподателя е била обявена за недопустима.

Визовата информационна система

Визовата информационна система (ВИС), също управлявана от eu-LISA, е разработена в подкрепа на прилагането на общата визова политика на ЕС[279]. ВИС позволява на страните от Шенген да обменят визови данни чрез система, която свързва консулствата на държавите от Шенген извън ЕС с външните гранично-пропускателни пунктове на всички шенгенски държави. ВИС обработва данни във връзка с молбите за краткосрочни визи за посещение или транзитно преминаване през Шенгенското пространство. ВИС позволява на граничните органи да проверяват чрез биометрични данни дали лицето, представящо визата, е нейният законен притежател, а също и да идентифицират лицата без или с фалшиви документи.

Съгласно Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета относно Визовата информационна система (ВИС) и обмена на данни между държави членки относно визите за краткосрочно пребиваване (*Регламент за ВИС*) само данни относно кандидата, неговите визи, снимки, дактилоскопични отпечатъци, връзки към предишни заявления за виза и досиета със заявленията на придружаващите го лица могат да бъдат записвани във ВИС[280]. Достъпът до ВИС с цел да се въвеждат, изменят или изтриват данни, се ограничава само до визовите органи на държавите членки, като се има предвид, че достъпът за преглед на данни се предоставя на визовите органи и на компетентните органите, отговарящи за проверките на външните гранично-пропускателни пунктове, имиграционните проверки и предоставянето на

279 Съвет на Европейския съюз (2004 г.), Решение 2004/512/ЕО на Съвета от 8 юни 2004 г. за създаване на Визова информационна система (ВИС), ОВ L 213, 15.6.2004 г.; Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. относно Визовата информационна система (ВИС) и обмена на данни между държави членки относно визите за краткосрочно пребиваване *(Регламент за ВИС)*, ОВ L 218, 13.8.2008 г.; Съвет на Европейския съюз (2008 г.), Решение 2008/633/ПВР на Съвета от 23 юни 2008 г. относно достъпа до Визовата информационна система (ВИС) за справки от оправомощени органи на държавите членки и от Европол с цел предотвратяване, разкриване и разследване на терористични действия и други тежки престъпления, ОВ L 218, 13.8.2008 г.

280 Член 5 от Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. относно Визовата информационна система (ВИС) и обмена на данни между държави членки относно визите за краткосрочно пребиваване (*Регламент за ВИС*), ОВ L 218, 13.8.2008 г.

убежище. При определени условия националните компетентни полицейски органи и Европол могат да поискат достъп до данни, въведени във ВИС, с цел предотвратяване, разкриване и разследване на терористични и криминални престъпления[281].

Евродак

Наименованието на Евродак се отнася до дактилоскопични, т.е. пръстови отпечатъци. Евродак е централизирана система, съдържаща дактилоскопични данни на граждани на трети държави, кандидатстващи за убежище в една от държавите членки на ЕС[282]. Системата е в действие от януари 2003 г. и нейната цел е да спомага за определянето на това, коя държава членка следва да отговаря за разглеждането на дадена молба за убежище съгласно Регламент (ЕО) № 343/2003 на Съвета за установяване на критерии и механизми за определяне на държава членка, компетентна за разглеждането на молба за убежище, която е подадена в една от държавите членки от гражданин на трета страна *(Регламент „Дъблин II“)*[283]. Личните данни в Евродак могат да се използват само с цел улесняване на прилагането на Регламент „Дъблин II“; всяко друго използване подлежи на санкциониране.

Евродак се състои от централно звено, управлявано от eu-LISA, за съхранение и съпоставяне на дактилоскопични отпечатъци и от система за електронно предаване на данни между държавите членки и централната база данни. Държавите членки взимат и предават дактилоскопичните отпечатъци на всеки гражданин на държава извън ЕС или на лице без гражданство на възраст поне 14 години, които потърсят убежище на тяхната територия или които са задържани за неразрешено преминаване на техните външни граници.

281 Съвет на Европейския съюз (2008 г.), Решение 2008/633/ПВР на Съвета от 23 юни 2008 г. относно достъпа до Визовата информационна система (ВИС) за справки от оправомощени органи на държавите членки и от Европол с цел предотвратяване, разкриване и разследване на терористични действия и други тежки престъпления, ОВ L 218, 13.8.2008 г.

282 Регламент (ЕО) № 2725/2000 на Съвета от 11 декември 2000 г. за създаване на система „Евродак“ за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Дъблинската конвенция, ОВ L 316, 15.12.2000 г.; Регламент (ЕО) № 407/2002 на Съвета от 28 февруари 2002 г. за определяне на някои условия за прилагането на Регламент (ЕО) № 2725/2000 относно създаването на системата „Евродак“ за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Дъблинската конвенция, ОВ L 62, 5.3.2002 г. *(регламентите за Евродак)*.

283 Регламент (ЕО) № 343/2003 на Съвета от 18 февруари 2003 г за установяване на критерии и механизми за определяне на държава членка, компетентна за разглеждането на молба за убежище, която е подадена в една от държавите членки от гражданин на трета страна, ОВ L 50, 25.2.2003 г. *(Регламент „Дъблин II“)*.

Освен това държавите членки могат да взимат и предават дактилоскопичните отпечатъци на граждани на държави извън ЕС или лица без гражданство, за които е установено, че пребивават на тяхната територия без разрешение.

Данните за дактилоскопични отпечатъци се съхраняват в базата данни на Евродак само под формата на псевдоними. В случай на съвпадение, псевдонимът, заедно с името на първата държава членка, която е предала данните за дактилоскопични отпечатъци, се разкрива на втората държава членка. Тази втора държава членка след това се обръща към първата държава членка, тъй като съгласно Регламент „Дъблин II" първата държава членка е отговорна за обработване на молбата за убежище.

Личните данни, съхранявани в Евродак, които се отнасят за лица, търсещи убежище, се запазват за срок от 10 години, считано от датата, на която са взети дактилоскопичните отпечатъци, освен когато физическото лице получи гражданство на държава членка на ЕС. В този случай данните трябва да бъдат изтривани незабавно. Данните, отнасящи се за чужди граждани, задържани заради неразрешено преминаване на външната граница, се съхраняват за срок от две години. Тези данни трябва да бъдат изтрити незабавно, ако физическото лице получи разрешително за пребиваване, напусне територията на ЕС или получи гражданство в държава членка.

Освен от всички държави членки на ЕС, Евродак се прилага също така и от Исландия, Норвегия, Лихтенщайн и Швейцария въз основа на международни споразумения.

EUROSUR

Европейската система за наблюдение на границите (*EUROSUR*)[284] е създадена с цел засилване на контрола на външните граници на Шенгенското пространство чрез разкриване, превенция и борба с незаконната имиграция и трансграничната престъпност. Нейната функция е засилване на информационния обмен и оперативното сътрудничество между националните координационни центрове и Frontex — агенцията на ЕС, отговорна за разработване и прилагане

284 Регламент (ЕС) № 1052/2013 на Европейския парламент и на Съвета от 22 октомври 2013 г. за създаване на Европейската система за наблюдение на границите (Eurosur), ОВ L 295, 6.11.2013 г.

на новото понятие „интегрирано управление на границите“[285]. Основните цели на системата са:

- намаляване на броя на незаконните мигранти, влизащи в ЕС, без да бъдат открити;
- намаляване на броя на смъртните случаи с незаконни мигранти чрез спасяване на повече човешки животи по море;
- увеличаване на вътрешната сигурност на ЕС като цяло чрез допринасяне за превенцията на трансграничната престъпност[286].

Тя започна да функционира на 2 декември 2013 г. във всички държави членки с външни граници и ще започне да функционира в другите държави от 1 декември 2014 г. Регламентът ще се прилага по отношение на наблюдението на сухопътните и морски външни граници и въздушните граници на държавите членки.

Митническа информационна система

Друга важна съвместна митническа система, създадена на равнище ЕС, е митническата информационна система (МИС)[287]. В процеса на установяване на вътрешен пазар всички проверки и формалности по отношение на стоки,

285 Регламент (ЕС) № 1168/2011 на Европейския парламент и на Съвета от 25 октомври 2011 г. за изменение на Регламент (ЕО) № 2007/2004 на Съвета за създаване на Европейска агенция за управление на оперативното сътрудничество по външните граници на държавите членки на Европейския съюз, ОВ L 394, 2011 г. (*Регламент относно Frontex*).

286 Виж също: Европейска комисия (2008 г.), Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален Комитет и Комитета на регионите — Относно проучване на създаването на Европейска система за наблюдение на границите (EUROSUR), COM(2008) 68 окончателен, Брюксел, 13 февруари 2008 г.; Европейска комисия (2011 г.), Оценка на въздействието, придружаваща предложението за регламент на Европейския парламент и на Съвета за създаване на Европейската система за наблюдение на границите (Eurosur), Работен документ на службите на Комисията, SEC(2011) 1536 окончателен, Брюксел, 12 декември 2011 г., стр. 18.

287 Съвет на Европейския съюз (1995 г.), Акт на Съвета от 26 юли 1995 г. за съставяне на Конвенцията за използване на информационните технологии за митнически цели, ОВ C 316, 27.11.1995 г., изменен от Съвета на ЕС през 2009 г., Регламент № 515/97 от 13 март 1997 г. относно взаимната помощ между административните органи на страните членки и сътрудничеството между тях и Комисията за осигуряване на правилното прилагане на митническото и селскостопанско законодателство, Решение 2009/917/ПВР на Съвета от 30 ноември 2009 г. относно използването на информационни технологии за митнически цели, ОВ L 323, 10.12.2009 г., Съвет на Европейския съюз (2009 г.) (*Решение за МИС*).

които се движат в рамките на територията на ЕС, бяха отменени, което доведе до повишен риск от измами. Този риск беше неутрализиран чрез засилено сътрудничество между митническите администрации на държавите членки. Целта на МИС е да подпомогне държавите членки при предотвратяването, разследването и наказателното преследване на сериозни нарушения на правото на ЕС в областта на митниците и селското стопанство.

Информацията, която се съдържа в МИС, включва лични данни във връзка със стоки, транспортни средства, стопански дейности, лица, стоки и парични средства, които са задържани, иззети или конфискувани. Тази информация може да се използва единствено за целите на наблюдението, докладването или извършването на специални проверки или за стратегически или оперативни анализи относно лица, за които има подозрение, че нарушават митническите разпоредби.

Достъп до МИС се предоставя на националните митнически, данъчни, селскостопански органи, органи по обществено здравеопазване и полицейски органи, както и Европол и Евроюст.

Обработването на лични данни трябва да бъде извършвано в съответствие със специфичните правила, установени в Регламент № 515/97, Конвенцията за МИС[288], както и в съответствие с разпоредбите на Директивата за защита на личните данни, Регламента относно защитата на данните при обработването им от институции на ЕС, Конвенция № 108 и Препоръката относно използването на данни в сектора на полицията. ЕНОЗД е отговорен за упражняване на надзора по съответствието на МИС с Регламент (ЕО) № 45/2001 и организира заседание поне веднъж в годината с всички национални надзорни органи за защита на данните, компетентни по въпросите на МИС.

288 *Пак там.*

8

Други специални европейски закони за защита на данните

ЕС	Обхванати въпроси	Съвет на Европа
Директива за защита на личните данни Директива за правото на неприкосновеност на личния живот и електронни комуникации	**Електронни комуникации**	Конвенция № 108 Препоръка относно телекомуникационните услуги
Директива за защита на личните данни, член 8, параграф 2, буква б)	**Трудови правоотношения**	Конвенция № 108 Препоръка относно трудовите правоотношения
		ЕСПЧ, Решение от 3 април 2007 г. по дело *Copland/Обединеното кралство*, № 62617/00
Директива за защита на личните данни, член 8, параграф 3	**Медицински данни**	Конвенция № 108 Препоръка относно медицинските данни
		ЕСПЧ, Решение от 25 февруари 1997 г. по дело *Z./Финландия*, № 22009/93
Директива относно клиничните изпитвания	**Клинични изпитвания**	
Директива за защита на личните данни, член 6, параграф 1, букви б) и д) и член 13, параграф 2	**Статистика**	Конвенция № 108 Препоръка относно статистическите данни

Регламент (ЕО) № 223/2009 относно европейската статистика Съд на ЕС, Решение от 16 декември 2008 г. по дело *Huber/Германия*, C-524/06	**Официална статистика**	Конвенция № 108 Препоръка относно статистическите данни
Директива 2004/39/ЕО относно пазарите на финансови инструменти Регламент (ЕС) № 648/2012 относно извънборсовите деривати, централните контрагенти и регистрите на транзакции Регламент (ЕО) № 1060/2009 относно агенциите за кредитен рейтинг Директива 2007/64/ЕО относно платежните услуги във вътрешния пазар	**Финансови данни**	Конвенция № 108 Препоръка № 90(19) относно защитата на личните данни, използвани за платежни и други свързани с това операции ЕСПЧ, Решение от 6 декември 2012 г. по дело *Michaud/Франция*, № 12323/11

В няколко случая на европейско равнище са били приети специални правни инструменти, чрез които общите правила на Конвенция № 108 или на Директивата за защита на личните данни се прилагат по-подробно за конкретни ситуации.

8.1. Електронни комуникации

Ключови въпроси

- В препоръка на Съвета на Европа от 1995 г. се съдържат специални правила относно защитата на личните данни в областта на телекомуникационните услуги и по-специално, телефонните услуги.
- В ЕС обработването на лични данни, отнасящи се до предоставянето на комуникационни услуги, е уредено в Директивата за правото на неприкосновеност на личния живот и електронни комуникации.
- Поверителността на електронните комуникации се отнася не само до съдържанието на съобщението, но и до данните за трафика, като информация за това с кого и кога е осъществена комуникацията и с каква продължителност е била тя, и данни за местонахождението, например откъде е осъществена комуникацията.

При комуникационните мрежи съществува по-висок риск от необоснована намеса в личния живот на потребителите, тъй като мрежите предоставят допълнителни технически възможности за подслушване и наблюдение на

комуникациите, осъществявани по тях. Логично е било счетено, че са необходими специални правила за защита на данните, за да се отговори на особените рискове за потребителите на комуникационни услуги.

През 1995 г. Съветът на Европа издаде Препоръка относно защита на личните данни в областта на телекомуникационните услуги и по-специално, телефонните услуги[289]. В съответствие с тази препоръка целите, за които се събират и обработват лични данни в контекста на телекомуникационните услуги, следва да се ограничават до свързването на потребителя с мрежата, предоставянето на самата телекомуникационна услуга, изготвянето на сметки, проверката, осигуряването на оптимално техническо функциониране и развитието на мрежата и услугите.

Специално внимание беше отделено също така на използването на комуникационните мрежи за изпращане на съобщения за директен маркетинг. Като общо правило не може да се изпращат съобщения за директен маркетинг на абонат, който изрично е отказал да получава рекламни съобщения. Автоматизирани повикващи устройства за предаване на предварително записани рекламни съобщения могат да се използват само ако абонатът е дал изрично съгласие. Националното законодателство трябва да предвижда подробни правила в тази област.

Що се касае до **правната рамка на ЕС**, след първи опит през 1997 г., през 2002 г. беше приета Директивата относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (*Директива за правото на неприкосновеност на личния живот и електронни комуникации*) и изменена през 2009 г. с цел **допълване и конкретизиране** на разпоредбите на Директивата за защита на личните данни за сектора на телекомуникациите[290]. Приложението на

289 Съвет на Европа, Комитет на министрите (1995 г.), Препоръка Rec(95)4 до държавите членки относно защитата на личните данни в областта на телекомуникационните услуги и по-специално телефонните услуги, 7 февруари 1995 г.

290 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации, ОВ L 201, 31.7.2002 г. (*Директива за правото на неприкосновеност на личния живот и електронни комуникации*), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите, ОВ L 337, 18.12.2009 г.

Директивата за правото на неприкосновеност на личния живот и електронни комуникации е ограничено до комуникационните услуги в обществените електронни мрежи.

В Директивата за правото на неприкосновеност на личния живот и електронни комуникации се разграничават три основни категории данни, създавани в процеса на комуникацията:

- данни, представляващи съдържанието на съобщенията, изпратени по време на комуникацията; тези данни са строго поверителни;

- данни, необходими за установяването и поддържането на комуникация, т. нар. данни за трафика, като информация за участниците в комуникацията, време и продължителност на комуникацията;

- в рамките на данните за трафика има данни, които се отнасят конкретно до местоположението на комуникационното устройство, т.нар. данни за местонахождението; тези данни същевременно са данни за местонахождението *на потребителите* на комуникационните устройства и са особено важни по отношение на потребителите на мобилни комуникационни устройства.

Данните за трафика могат да се използват от доставчика на услуги само с цел изготвяне на сметка и за техническо предоставяне на услугата. Със съгласието на заинтересованото лице, обаче, тези данни могат да бъдат разкривани на други администратори на данни, които предлагат услуги с добавена стойност, като предоставяне на свързана с местонахождението на потребителя информация за най-близката станция на метрото или аптека или прогнозата за времето за това място.

За друг достъп до данните за комуникациите в електронните мрежи, например достъпа за целите на разследването на престъпления, в съответствие с член 15 трябва да са спазени изискванията за обоснована намеса в правото на защита на личните данни, както е постановено в член 8, параграф 2 от ЕКПЧ и потвърдено от Хартата в нейните членове 8 и 52.

С измененията от 2009 г. в Директива за правото на неприкосновеност на личния живот и електронни комуникации[291] се въведе следното:

- Ограниченията за изпращането на електронна поща за целите на директния маркетинг се разпростират върху кратките съобщения (SMS), мултимедийните услуги (MMS) и други видове подобни приложения; изпращането на електронна поща за целите на маркетинга е забранено освен ако не е получено предварително съгласие. Без такова съгласие електронна поща за маркетингови цели може да се адресира само до предишни клиенти, ако те са предоставили адреса на своята електронна поща и не възразяват на това.

- На държавите членки се възлага задължението да предвидят средства за правна защита срещу нарушения на забраната за изпращане на нежелани съобщения[292].

- Инсталирането на „бисквитки“ (cookies) на компютъра — софтуер, който наблюдава и записва действията на използващия го, вече не е позволено без неговото съгласие. Националното законодателство следва да регламентира по-подробно начините, по които следва да се изрази и получи съгласието, за да предложи достатъчна защита[293].

Ако има нарушение на сигурността на данните в резултат на неразрешен достъп, загуба или унищожаване на лични данни, компетентният надзорен орган трябва да бъде уведомен незабавно. Абонатите трябва да бъдат информирани, ако е възможно да понесат щети като последица от нарушаването на сигурността на данните[294].

---

291 Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите, ОВ L 337, 18.12.2009 г.

292 Вж. изменената директива, член 13.

293 Вж. *пак там*, член 5, вж. също Работна група за защита на личните данни по член 29 (2012 г.), *Становище 04/2012 относно освобождаването от изискването за съгласие за някои „бисквитки“*, WP 194, Брюксел, 7 юни 2012 г.

294 Вж. също така Работна група за защита на личните данни по член 29 (2011 г.), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* [*Работен документ № 01/2011 относно действащата нормативна уредба на ЕС в областта на нарушения по отношение на личните данни и препоръки за бъдещи развития на политиката*], WP 184, Брюксел, 5 април 2011 г.

Директивата за запазване на лични данни[295] (произнесена за невалидна на 08 април 2014 г.), задължаваше доставчиците на съобщителни услуги да запазват данни за трафика, по-специално, за целите на борбата с тежките престъпления, за срок от най-малко шест месеца и най-много 24 месеца, независимо от това дали доставчикът все още е имал нужда от тези данни за изготвяне на абонатни сметки или за техническо предоставяне на услугата.

Държавите членки на ЕС, назначават независими публични органи, които отговарят за наблюдението на сигурността на запазените данни.

Запазването на телекомуникационни данни очевидно представлява намеса в правото на защита на данните[296]. Дали тази намеса е обоснована или не е било предмет на спор в няколко съдебни производства в държави членки на ЕС[297].

Пример: In *Digital Rights, Ирландия и Seitlinger и други*[298], СЕС обяви, че Директивата за задържане на данни е невалидна. Съгласно Съда, *„широко мащабната и определено сериозна намеса на директивата в основните права не е достатъчно обоснована, за да гаранитра, че тази намеса всъщност е достатъчно ограничена.*

Решаващ въпрос в контекста на електронните комуникации е намесата от страна на публичните органи. Способите за наблюдение или прихващане на комуникации, като например устройствата за подслушване или записване, са позволени само ако това е предвидено от закона и ако представлява необходима мярка в демократичното общество в интерес на защитата на

295 Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, ОВ L 105, 13.4.2006 г.

296 ЕНОЗД (2011 г.), *Становище на Европейския надзорен орган по защита на данните (ЕНОЗД) от 31 май 2011 г. относно доклада на Комисията до Съвета и Европейския парламент за оценка на директивата за запазване на данни (Директива 2006/24/ЕО)*, 31 май 2011 г.

297 Германия, Федерален конституционен съд (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 март 2010 г.; Румъния, Конституционен съд (*Curtea Constituțională a României*), № 1258, 8 октомври 2009 г.; Чешката република, Конституционен съд (*Ústavní soud České republiky*), 94/2011 Сб., 22 март 2011 г.

298 СЕС, Съединени дела C-293/12 и C-594/12, *Digital Rights Ирландия и Seitlinger и други,* 8 април 2014 г., параграф 65.

държавната сигурност, обществената безопасност, паричните интереси на държавата или борбата с престъпленията.

Пример: По делото *Malone/Обединеното кралство*[299] жалбоподателят е обвинен в редица престъпления, отнасящи се до недобросъвестно търгуване с откраднати стоки. По време на процеса става известно, че телефонен разговор на жалбоподателя е бил прихванат на основание на заповед, издадена от държавния секретар на Министерството на вътрешните работи. Макар че начинът, по който комуникациите на жалбоподателя са били прихванати, е бил законен от гледна точка на националното право, ЕСПЧ е установил, че не са били налице законови правила относно обхвата и начина на упражняване на правото на преценка, което са имали публичните органи в тази област, и че следователно намесата, произтичаща от съществуването на въпросната практика, не е била „в съответствие със закона". Съдът е постановил, че е налице нарушение на член 8 от ЕКПЧ.

8.2. Данни за заетостта

Ключови въпроси

- Специални правила за защита на данните при трудови правоотношения се съдържат в Препоръката на Съвета относно данните за заетостта.
- В Директивата за защита на личните данни трудовите правоотношения се посочват по-специално само в контекста на обработването на чувствителни данни.
- Валидността на съгласието, което трябва да е било изразено свободно, като правно основание за обработването на данни може да е съмнителна, като се има предвид икономическата неравнопоставеност между работодателя и служителите. Обстоятелствата, при които е дадено съгласието, трябва да бъдат внимателно оценени.

В ЕС не съществува специална правна рамка, уреждаща обработването на данните в контекста на трудовите правоотношения. В Директивата за защита на личните данни трудовите правоотношения се посочват по-специално само в член 8, параграф 2 от директивата, който се отнася до обработването на

299 ЕСПЧ, Решение от 26 април 1985 г. по дело *Malone/Обединеното кралство*, № 8691/79.

чувствителни данни. Що се отнася до Съвета на Европа — Препоръката относно данните за заетостта е издадена през 1989 г. и в момента се актуализира[300].

В работен документ на Работната група по член 29 е включено проучване на най-често срещаните проблеми, свързани със защитата на данните, характерни за областта на трудовите правоотношения[301]. Работната група е анализирала значението на съгласието като правно основание за обработването на данни за заетостта[302]. Тя е констатирала, че икономическата неравнопоставеност между работодателя, търсещ съгласие, и служителят, който дава такова, често поражда съмнения дали съгласието е било изразено свободно или не. Следователно обстоятелствата, при които се търси съгласие, следва да бъдат внимателно разгледани при оценяването на валидността на съгласието в контекста на трудовите правоотношения.

Често срещан проблем със защитата на данните в днешната типична работна среда е доколко е законосъобразно следенето на електронните комуникации на служителите на работното място. Често се твърди, че този проблем може лесно да бъде решен, като се забрани използването по време на работа на средствата за комуникация за лични цели. Подобна обща забрана обаче може да бъде несъразмерна и нереалистична. От особен интерес в този контекст е следното съдебно решение на ЕСПЧ:

Пример: В дело *Copland/Обединеното кралство*[303] използването на телефона, електронната поща и интернет от страна на служителка на колеж е било следено тайно, за да се установи дали е прекалявала с използването на оборудването на колежа за лични цели. ЕСПЧ е постановил, че

300 Съвет на Европа, Комитет на министрите (1989 г.), Препоръка Rec(89)2 до държавите членки относно защитата на лични данни, използвани за целите на трудови правоотношения, 18 януари 1989 г. Вж. още Консултативния комитет към Конвенция № 108, Проучване относно Препоръка R (89) 2 относно защитата на лични данни, използвани за целите на трудови правоотношения и с цел предлагане на предложения за преразглеждане на горепосочената препоръка, 9 септември 2011 г.

301 Работна група за защита на личните данни по член 29 (2001 г.), *Opinion 8/2001 on the processing of personal data in the employment context [Становище 8/2001 относно обработването на личните данни в контекста на трудовите правоотношения]*, WP 48, Брюксел, 13 септември 2001 г.

302 Работна група за защита на личните данни по член 29 (2005 г.), *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995 [Работен документ за общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г.]*, WP 114, Брюксел, 25 ноември 2005 г.

303 ЕСПЧ, Решение от 3 април 2007 г. по дело *Copland/Обединеното кралство*, № 62617/00.

обажданията по телефона от служебното място се обхващат от понятията личен живот и лична кореспонденция. Следователно подобни обаждания и електронни съобщения, изпратени от работното място, както и информацията, произтичаща от следенето на личното използване на интернет, са защитени по силата на член 8 от ЕКПЧ. В случая на жалбоподателката не са били налице никакви разпоредби, уреждащи обстоятелствата, при които работодателите могат да следят използването на телефона, електронната поща и интернет от страна на служителите. Следователно намесата не е била в съответствие със закона. Съдът е заключил, че е налице нарушение на член 8 от ЕКПЧ.

Съгласно Препоръката на Съвета на Европа за данните за заетостта, личните данни, събирани за целите на трудовите правоотношения, следва да бъдат получавани пряко от самия служител.

Личните данни, събирани с цел наемане на работа, трябва да се ограничават до информацията, необходима за оценка на пригодността на кандидатите и техния потенциал за професионално развитие.

В препоръката специално се споменава за данните, събирани с цел оценка на работата или потенциала на отделните служители. Данните от тази субективна преценка трябва да се основават на добросъвестни и безпристрастни оценки и начинът, по който са формулирани, не трябва да е оскърбителен. Това се изисква в съответствие с принципите за добросъвестно обработване и за точност на данните.

Особен аспект на правото за защита на данните при взаимоотношенията работодател — служител е ролята на представителите на служителите. Тези представители могат да получават лични данни на служителите само доколкото това е необходимо, за да бъдат представениинтересите на служителите.

Чувствителните лични данни, събирани за целите на трудовите правоотношения, могат да бъдат обработвани само в определени случаи и при спазване на гаранциите, залегнали в националното право. Работодателите могат да искат от служителите или кандидатите за работа информация за здравословното им състояние или да ги подлагат на медицински изследвания само, ако това е необходимо за определяне на пригодността им за съответната работа, за изпълняване на изискванията на профилактичната медицина или за целите на отпускане на социални обезщетения. Данни за здравето не могат да се

събират от други източници освен от съответния служител след получаване на изрично и информирано съгласие или когато националното законодателство предвижда това.

Съгласно Препоръката относно данните за заетостта служителите следва да бъдат информирани за целите на обработването на личните им данни, вида на съхраняваните лични данни, субектите, на които редовно се предават данните, целите на подобно предаване и правното му основание. Работодателите следва също предварително да осведомяват своите служители, ако въвеждат или адаптират автоматизирани системи за обработването на личните им данни или ако следят дейностите или производителността на служителите.

Служителите трябва да имат право на достъп до своите данни за заетостта, както и право на коригиране или изтриване. Освен това, служителите трябва да имат право да оспорват извършена преценка на тяхната работа, направена въз основа на обработване на лични данни. Тези права обаче могат да бъдат временно ограничавани за целите на вътрешни разследвания. Ако на служител бъде отказан достъп, коригиране или изтриване на лични данни за заетостта, националното право трябва да предвижда подходящи процедури за оспорване на този отказ.

8.3. Медицински данни

Ключов въпрос

- Медицинските данни са чувствителни данни и следователно са обект на специална защита.

Личните данни, отнасящи се до здравословното състояние на съответното физическо лице, се определят като чувствителни данни съгласно член 8, параграф 1 от Директивата за защита на личните данни и член 6 от Конвенция № 108. От своя страна, медицинските данни подлежат на по-строг режим на обработване от нечувствителните данни.

Пример: В дело *Z./Финландия*[304] бившият съпруг на жалбоподателката, заразен с ХИВ, е бил извършил редица сексуални престъпления. Впоследствие той е бил осъден за убийство по непредпазливост на основание на това, че умишлено е изложил своите жертви на опасност от заразяване с ХИВ. Националният съд е определил пълното съдебно решение и документите по делото да останат поверителни за срок от 10 години въпреки молбите на жалбоподателката за по-дълъг период на поверителност. Тези молби са били отхвърлени от апелативния съд и неговото решение е съдържало пълните имена както на жалбоподателката, така и на бившия ѝ съпруг. ЕСПЧ е постановил, че намесата не е била счетена за необходима в едно демократично общество, тъй като защитата на медицинските данни е била от първостепенно значение за упражняване на правото на зачитане на личния и семейния живот, по-специално по отношение на информацията за заразяване с ХИВ, като се има предвид заклеймяването на това заболяване в много общества. Ето защо съдът е заключил, че предоставянето на достъп до самоличността и медицинското състояние на жалбоподателката, така както е описано в решението на апелативния съд, след само 10 години след произнасянето на решението е в нарушение на член 8 от ЕКПЧ.

В член 8, параграф 3 от Директивата за защита на личните данни се позволява обработването на медицински данни, когато то „е необходимо за целите на профилактичната медицина, поставяне на медицинска диагноза, предоставяне на грижи или лечение, или за управлението на здравни служби". Обработването е допустимо обаче само когато се извършва от медицинско лице, което е длъжно да спазва професионална тайна, или от друго лице, което е също обвързано с равностойно задължение[305].

В Препоръката относно медицинските данни на Съвета на Европа от 1997 г. се прилагат по-подробно принципите на Конвенция № 108 за обработването на данни от медицинско естество[306]. Предложените правила са в съответствие

304 ЕСПЧ, Решение от 25 февруари 1997 г. по дело *Z./Финландия*, № 22009/93, точки 94 и 112; вж. също ЕСПЧ, Решение от 27 август 1997 г. по дело *M.S./Швеция*, № 20837/92; ЕСПЧ, Решение от 10 октомври 2006 г. по дело *L.L./Франция*, № 7508/02; ЕСПЧ, Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03; ЕСПЧ, Решение от 28 април 2009 г. по дело *K.H и други/Словакия*, № 32881/04; ЕСПЧ, Решение от 2 юни 2009 г. по дело *Szuluk/Обединеното кралство*, № 36936/05.

305 Вж. също ЕСПЧ, Решение от 25 ноември 2008 г. по дело *Biriuk/Литва*, № 23373/03.

306 Съвет на Европа, Комитет на министрите (1997 г.), Препоръка Rec(97)5 до държавите членки относно защитата на медицински данни, 13 февруари 1997 г.

с тези от Директивата за защита на личните данни по отношение на законосъобразните цели на обработването на медицински данни, необходимите задължения за опазване на професионална тайна от страна на лицата, служещи си със здравните данни, и правата на съответните физически лица за прозрачност и достъп, коригиране и изтриване. Освен това медицинските данни, обработвани законосъобразно от здравни специалисти, не могат да бъдат предавани на правоприлагащи органи освен ако не бъдат предоставени „достатъчни гаранции за предотвратяване на разкриване, несъвместимо със зачитането на [...] личния живот, гарантиран съгласно член 8 от ЕКПЧ“[307].

Също така, в Препоръката относно медицинските данни се съдържат специални разпоредби относно медицинските данни на неродени деца и недееспособни лица и относно обработването на генетични данни. Научните изследвания се признават изрично като основание за по-дългосрочно от необходимото съхранение на данните, въпреки че това обикновено изисква анонимизиране. В член 12 от Препоръката относно медицинските данни се предлагат подробни разпоредби за случаи, при които изследователите се нуждаят от лични данни и анонимизираните данни са недостатъчни.

Използването на псевдоним може да бъде подходящ начин за задоволяване на нуждите на науката и същевременно за защита на интересите на съответните пациенти. Концепцията за използването на псевдоним в контекста на защитата на данните е обяснена по-подробно в раздел 2.1.3.

На национално и европейско равнище са в ход интензивни дискусии по инициативи за съхранение на данни за медицинското лечение на даден пациент в електронно здравно досие[308]. Специален аспект на наличието на национални системи за електронни здравни досиета е възможността за трансграничен достъп до тях — една тема, която е от особен интерес в ЕС в контекста на трансграничните здравни грижи[309].

Друга дискутирана област във връзка с новите разпоредби са клиничните изпитвания или изпитването на нови лекарствени продукти върху пациенти в

307 ЕСПЧ, Решение от 6 юни 2013 г. по дело *Avilkina и други/Русия*, № 1585/09, точка 53 (неокончателно).

308 Работна група за защита на личните данни по член 29 (2007 г.), *Работен документ относно обработването на лични здравни данни в електронните здравни досиета (ЕЗД)*, WP 131, Брюксел, 15 февруари 2007 г.

309 Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011 г. за упражняване на правата на пациентите при трансгранично здравно обслужване, ОВ L 88, 4.4.2011 г.

документирана среда на изследване. Тази тема има също значителни последици върху защитата на данните. Клиничните изпитвания на лекарствени продукти за хуманна употреба се уреждат с Директива 2001/20/ЕО на Европейския парламент и на Съвета от 4 април 2001 г. относно сближаване на законовите, подзаконовите и административните разпоредби на държавите членки относно прилагането на добрата клинична практика при провеждането на клинични изпитвания на лекарствени продукти за хуманна употреба (*Директива относно клиничните изпитвания*)[310]. През декември 2012 г. Европейската комисия предложи регламент, който да замени Директивата относно клиничните изпитвания, с цел процедурите за изпитване да станат по-уеднаквени и ефективни[311].

Има много други предстоящи законодателни и други инициативи на равнището на ЕС по отношение на личните данни в сектора на здравеопазването[312].

8.4. Обработване на данни за статистически цели

Ключови въпроси

- Данните, събирани за статистически цели, не могат да се използват за каквито и да било други цели.
- Данните, събирани законно с каквато и да било цел, не могат да се използват в бъдещи периоди за статистически цели, при условие че националното законодателство предвижда адекватни гаранции, които се изпълняват от потребителите. За тази цел следва да бъде предвидено по-специално анонимизирането или използването на псевдоним преди предаването на данните на трети лица.

310 Директива 2001/20/ЕО на Европейския парламент и на Съвета от 4 април 2001 г. относно сближаване на законовите, подзаконовите и административните разпоредби на държавите членки относно прилагането на добрата клинична практика при провеждането на клинични изпитвания на лекарствени продукти за хуманна употреба, ОВ L 121, 1.5.2001 г.

311 Европейска комисия (2012 г.), *Предложение за регламент на Европейския парламент и на Съвета относно клиничните изпитвания на лекарствени продукти за хуманна употреба, и за отмяна на Директива 2001/20/ЕО*, COM(2012) 369 окончателен, Брюксел, 17 юли 2012 г.

312 ЕНОЗД (2013 г.), *Становище на Европейския надзорен орган по защита на данните относно съобщението на Комисията „План за действие за електронно здравеопазване за периода 2012—2020 година — иновационно здравно обслужване през 21-ви век“*, Брюксел, 27 март 2013 г.

В Директивата за защита на личните данни обработването на данни за статистически цели се посочва в контекста на възможни изключения от принципите относно защитата на данните. В член 6, параграф 1, буква б) от директивата принципът за ограничаване на целта може да не бъде спазен съгласно националното законодателство в полза на бъдещо използване на данните за статистически цели, въпреки че в националното законодателство също така трябва да бъдат предвидени всички необходими гаранции. Член 13, параграф 2 от директивата позволява ограничения на правата на достъп от националното законодателство, ако данните се обработват единствено и само за статистически цели; въпреки това в националното законодателство трябва да съществуват адекватни гаранции. В този контекст, Директивата за защита на личните данни предвижда конкретно изискване за това, че никаква част от данните, придобити или създадени в хода на статистическо изследване, не могат да бъдат използвани за конкретни решения относно физическите лица.

Въпреки че данните, които са били законосъобразно събрани от администратор за някаквацел, могат да бъдат повторно използвани от този администратор за негови собствени статистически цели — т.нар. вторична статистика — данните би трябвало да бъдат анонимизирани или псевдонимизирани, в зависимост от контекста,преди предаването им на трето лице за статистически цели, освен когато физическото лице се е съгласило с това или то е изрично предвидено в националното законодателство. Това произтича от изискването за подходящи гаранции съгласно член 6, параграф 1, буква б) от Директивата за защита на личните данни.

Най-важните случаи, при които се използват данни за статистически цели, са официалните статистически изследвания, извършвани от националните статистически бюра и статистическите бюра на ЕС въз основа на националните закони и разпоредбите на ЕС относно официалната статистика. Според тези закони и разпоредби гражданите и предприятията обикновено се задължават да разкриват данните на статистическите органи. Длъжностните лица, които работят в статистическите бюра, са обвързани от специални задължения за опазване на професионална тайна, които се спазват стриктно, тъй като те са от съществено значение за високото ниво на доверие у гражданите, което е необходимо, ако данните ще се предоставят на статистическите органи.

Регламент (ЕО) № 223/2009 относно европейската статистика (*Регламент относно европейската статистика*) съдържа съществени правила за защитата на данните при извършването на официални статистически изследвания

и по тази причина може също така да бъде считан за приложим, що се отнася до разпоредбите относно официалните статистически изследвания на национално равнище[313]. В регламента се поддържа принципът, че е необходимо достатъчно точно право основание за извършването на официални статистически операции[314].

Пример: По делото *Huber/Германия*[315] Съдът на ЕС е установил, че събирането и съхранението на лични данни от даден орган за статистически цели само по себе си не е представлявало достатъчно основание за това обработването да е законосъобразно. Било е необходимо законът, който предвижда обработването на лични данни, също да отговаря на изискването за необходимост, но случаят не е бил такъв в дадения контекст.

По отношение на Съвета на Европа — през 1997 г. беше издадена Препоръката относно статистическите данни, която обхваща извършването на статистически изследвания в публичния и частния сектор[316]. С Препоръката бяха въведени принципи, които съвпадат с основните правила на Директивата за защита на личните данни, описани по-горе. Предвидени са по-подробни правила по следните въпроси.

Докато данните, събирани от администратора за статистически цели не могат да бъдат използвани за други цели, данните, които не са събирани за предоставяне на статистика, могат да бъдат използвани по-нататък за такава цел. Препоръката относно статистическите данни дори дава възможност за съобщаване на данни на трети лица, ако това се извършва само за статистически

313 Регламент (ЕО) № 223/2009 на Европейския парламент и на Съвета от 11 март 2009 г. относно европейската статистика и за отмяна на Регламент (ЕО, Евратом) № 1101/2008 за предоставянето на поверителна статистическа информация на Статистическата служба на Европейските общности, на Регламент (ЕО) № 322/97 на Съвета относно статистиката на Общността и на Решение 89/382/ЕИО, Евратом на Съвета за създаване на Статистически програмен комитет на Европейските общности, ОВ L 87, 31.3.2009 г.

314 Този принцип предстои да бъде по-подробно описан в Кодекса на европейската статистическа практика, който в съответствие с член 11 от Регламента относно европейската статистика предоставя етични насоки относно това как да се извършват официалните статистически изследвания, включително и относно внимателното използване на лични данни; Кодексът е достъпен на адрес: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 Съд на ЕС, Решение от 16 декември 2008 г. по дело *Huber/Bundesrepublik Deutschland*, C-524/06, вж. по-специално точка 68.

316 Съвет на Европа, Комитет на министрите (1997 г.), Препоръка Rec(97)18 до държавите членки относно защитата на лични данни, събирани и обработвани за статистически цели, 30 септември 1997 г.

цели. В такива случаи, лицата следва да се договорят и писмено да определят обхвата на по-нататъшното законно използване на данните за статистически цели. Тъй като това не може да бъде заместител на съгласието на физическото лице, следва да се приеме, че в националното законодателство трябва да са предвидени допълнителни подходящи гаранции, за да се намалят рисковете от злоупотреба с лични данни, като например задължение за анонимизиране на данните или представянето им чрез използване на псевдоним преди тяхното предаване.

Хората, които професионално се занимават със статистически изследвания, следва да бъдат обвързани със специални задължения за опазване на професионална тайна — каквато е обичайната практика в сферата на официалната статистика — съгласно националното законодателство. Това задължение следва да бъде разширено също и до анкетьорите, ако те се занимават със събиране на данни от съответните физически лица или от други лица.

Ако статистическо проучване, в което се използват лични данни, не е предвидено от закона, съответните физически лица ще трябва да дадат съгласието си за използването на техните данни, за да стане то законно, или на тях поне следва да им да се даде възможност да изразят възражение. Ако личните данни се събират за статистически цели чрез интервюиране на лица, тези лица трябва да бъдат ясно информирани за това дали разкриването на данните е задължително съгласно националното законодателство или не. Чувствителни данни никога не следва да се събират по такъв начин, че дадено лице да може да бъде идентифицирано, освен ако това не е изрично разрешено от националното законодателство.

Когато дадено статистическо проучване не може да бъде извършено без анонимизирани данни и наличието на лични данни наистина е необходимо, събраните за тази цел данни следва да бъдат анонимизирани възможно най-скоро. Резултатите от статистическото проучване не трябва да дават ни най-малка възможност за идентифициране на съответните физически лица, освен ако това очевидно не би породило никакъв риск.

След приключването на статистическия анализ използваните лични данни следва да бъдат изтрити или анонимизирани. В този случай в Препоръката относно статистическите данни се предлага идентификационните данни да бъдат съхранявани отделно от другите лични данни. Това означава, например, че данните следва или да бъдат представени чрез използване на псевдоним,

или ключът за шифроване или списъкът с идентификационните синоними следва да се съхранява отделно отпсевдонимизираните.

8.5. Финансови данни

Ключови въпроси

- Въпреки че финансовите данни не са чувствителни данни по смисъла на Конвенция № 108 или Директивата за защита на личните данни, тяхното обработване се нуждае от особени гаранции за осигуряване на точност и сигурност на данните.
- Електронните платежни системи е нужно да разполагат с вградена защита на данните — така наречената защита на данните още при проектирането.
- В тази област възникват особени проблеми със защитата на данните поради нуждата от наличието на подходящи механизми за автентификация.

Пример: В дело *Michaud/Франция*[317] жалбоподателят, френски адвокат, е оспорил задължението си по силата на френското законодателство да съобщава, ако има подозрения за възможни дейности на негови клиенти, свързани с изпиране на пари. ЕСПЧ е отбелязал, че изискването адвокати да съобщават на административните органи информация относно друго лице, която е станала тяхно достояние вследствие на контакт с това лице, е намеса в правото на адвоката да се зачитат неговата кореспонденция и личният му живот по силата на член 8 от ЕКПЧ, тъй като тази концепция обхваща дейности от професионално или служебно естество. Намесата обаче е била законосъобразна и е преследвала законна цел, а именно предотвратяването на безредици и престъпления. Тъй като адвокатите са задължени да съобщават за подозрения само при много ограничени обстоятелства, ЕСПЧ е постановил, че това задължение е било съразмерно, и е заключил, че не е било налице нарушение на член 8.

Прилагането на общата правна рамка за защита на данните по отношение на плащанията, така както се съдържа в Конвенция № 108, е развито от Съвета

317 ЕСПЧ, Решение от 6 декември 2012 г. по дело *Michaud/Франция*, № 12323/11; вж. също ЕСПЧ, Решение от 16 декември 1992 г. по дело *Niemitz/Германия*, № 13710/88, точка 29; и ЕСПЧ, Решение от 25 юни 1997 г. по дело *Halford/Обединеното кралство*, № 20605/92, точка 42.

на Европа в Препоръка Rec(90)19 от 1990 г.[318] В нея се изяснява обхватът на законосъобразното събиране и използване на данни заплащанията, по-специално чрез разплащателни карти. Освен това на националните законодатели се предлагат подробни разпоредби за ограниченията за предаване на трети страни на данни за плащанията, за сроковете за съхранение на данните, за прозрачността, сигурността на данните и трансграничното предоставяне на данни, и накрая, за надзора и средствата за правна защита. Предложените решения съответстват на това, което впоследствие е предвидено като обща рамка на ЕС за защита на данните в Директивата за защита на личните данни.

В момента се създават редица правни инструменти за регулиране на пазарите на финансови инструменти и дейностите на кредитните институции и инвестиционните посредници[319]. Други правни инструменти подпомагат борбата със злоупотребата с вътрешна информация и с манипулирането на пазарите[320]. Най-критичните въпроси в тези области, оказващи въздействие върху защитата на данните, са:

- съхранението на документацията за финансовите сделки;
- трансферът на лични данни към трети държави;

318 Съвет на Европа, Комитет на министрите (1990 г.), Препоръка № R (90) 19 относно защитата на личните данни, използвани за платежни и други свързани с това операции, 13 септември 1990 г.

319 Европейска комисия (2011 г.), *Предложение за директива на Европейския парламент и на Съвета относно относно пазарите на финансови инструменти и за отмяна на Директива 2004/39/ЕО на Европейския парламент и на Съвета*, COM(2011) 656 окончателен, Брюксел, 20 октомври 2011 г.; Европейска комисия (2011 г.), *Предложение за регламент на Европейския парламент и на Съвета относно пазарите на финансови инструменти и за изменение на регламента [EMIR] за извънборсовите деривати, централните контрагенти и регистрите на трансакции*, COM(2011) 652 окончателен, Брюксел, 20 октомври 2011 г.; Европейска комисия (2011 г.), *Предложение за директива на Европейския парламент и на Съвета относно лицензирането и осъществяването на дейността на кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници и за изменение на Директива 2002/87/ЕО на Европейския парламент и на Съвета относно допълнителния надзор на кредитните институции, застрахователните предприятия и на инвестиционните посредници към един финансов конгломерат*, COM(2011) 453 окончателен, Брюксел, 20 октомври 2011 г.

320 Европейска комисия (2011 г.), *Предложение за регламент на Европейския парламент и на Съвета относно злоупотребата с вътрешна информация и манипулирането на пазара (пазарна злоупотреба)*, COM(2011) 651 окончателен, Брюксел, 20 октомври 2011 г.; Европейска комисия (2011 г.), *Предложение за директива на Европейския парламент и на Съвета относно наказателните санкции за злоупотреба с вътрешна информация и манипулиране на пазара*, COM(2011) 654 окончателен, Брюксел, 20 октомври 2011 г.

- записването на телефонни разговори или електронни съобщения, включително правомощията на компетентните органи да изискват телефонни записи и сведения за преноса на данни;

- оповестяването на лични данни, включително публикуването на санкции;

- надзорните и разследващите правомощия на компетентните органи, включително проверки на място и навлизане в частни обекти за изземване на документи;

- механизмите за докладване за нарушения, т.е. схеми за подаване на сигнали за корупция; и

- сътрудничеството между компетентните органи на държавите членки и Европейския орган за ценни книжа и пазари (ESMA).

В тези области има и други въпроси, които се решават специално, включително събирането на данни за финансовото състояние на съответните физически лица — субекти на данните[321], или трансграничното плащане чрез банкови преводи, което неизбежно води до движение налични данни[322].

321 Регламент (ЕО) № 1060/2009 на Европейския парламент и на Съвета от 16 септември 2009 г. относно агенциите за кредитен рейтинг, ОВ L 302, 17.11.2009 г.; Европейска комисия, *Предложение за регламент на Европейския парламент и на Съвета за изменение на Регламент (ЕО) № 1060/2009 относно агенциите за кредитен рейтинг*, COM(2010) 289 окончателен, Брюксел, 2 юни 2010 г.

322 Директива 2007/64/ЕО на Европейския парламент и на Съвета от 13 ноември 2007 г. относно платежните услуги във вътрешния пазар, за изменение на директиви 97/7/ЕО, 2002/65/ЕО, 2005/60/ЕО и 2006/48/ЕО и за отмяна на Директива 97/5/ЕО, ОВ L 319, 5.12.2007 г.

Допълнителна литература

Глава 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Brussels, достъпно на: www.edri.org/files/paper06_datap.pdf.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussels, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, No. 5, pp. 281–288.

Warren, S. and Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review,* Vol. 4, No. 5, pp. 193–220, достъпно на адрес: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Глава 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. and Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, Vol. 57, No. 6, pp. 1701–1777.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*, достъпно на: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Глави 3—5

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' в: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II) [„Защита на данните в Европейския съюз: ролята на националните органи за защита на данните" (Укрепване на структурата на основните права в ЕС II)]*,Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union [Разработване на индикатори за защитата, зачитането и насърчаването на правата на детето в Европейския съюз]* (Conference edition), Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, достъпно на: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Глава 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Глава 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office, достъпно на: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* ERA Forum, Vol. 13, No. 3, pp. 381–395.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the

Law of External Relations, CLEER Working Papers 2013/2, достъпно на: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Глава 8

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Съдебна практика

Избрана съдебна практика на Европейския съд по правата на човека

Достъп до лични данни

Решение от 7 юли 1989 г. по дело *Gaskin/Обединеното кралство*, № 10454/83
Решение от 25 септември 2012 г. по дело *Godelli/Италия*, № 33783/09
Решение от 28 април 2009 г. по дело *K.H и други/Словакия*, № 32881/04
Решение от 26 март 1987 г. по дело *Leander/Швеция*, № 9248/81
Решение от 13 февруари 2003 г. по дело *Odièvre/Франция* [голям състав], № 42326/98

Балансиране на защитата на данните със свободата на изразяване на мнение

Решение от 7 февруари 2012 г. по дело *Axel Springer AG/Германия* [голям състав], № 39954/08
Решение от 24 юни 2004 г. по дело *Von Hannover/Германия*, № 59320/00
Решение от 7 февруари 2012 г. по дело *Von Hannover/Германия (№ 2)* [голям състав], № 40660/08 и 60641/08

Предизвикателства в областта на защитата на данни онлайн

Решение от 2 декември 2008 г. по дело *K.U./Финландия*, № 2872/02

Кореспонденция

Решение от 16 февруари 2000 г. по дело *Amann/Швейцария* [голям състав], № 27798/95
Решение от 14 март 2013 г. по дело *Bernh Larsen Holding AS и други/Норвегия*, № 24117/08
Решение от 18 ноември 2008 г. по дело *Cemalettin Canli/Турция*, № 22427/04
Решение от 2 февруари 2010 г. по дело *Dalea/Франция*, № 964/07
Решение от 7 юли 1989 г. по дело *Gaskin/Обединеното кралство*, № 10454/83
Решение от 27 октомври 2009 г. по дело *Haralambie /Румъния*, № 21737/03
Решение от 18 октомври 2011 г. по дело *Khelili/Швейцария*, № 16188/07
Решение от 26 март 1987 г. по дело *Leander/Швеция*, № 9248/81
Решение от 26 април 1985 г. по дело *Malone/Обединеното кралство*, № 8691/79
Решение от 24 февруари 1995 г. по дело *McMichael/Обединеното кралство*, № 16424/90
Решение от 24 септември 2002 г. по дело *M.G./Обединеното кралство*, № 39393/98
Решение от 4 май 2000 г. по дело *Rotaru/Румъния*, [голям състав], № 28341/95
Решение от 4 декември 2008 г. по дело *S. и Marper/Обединеното кралство*, № 30562/04 и 30566/04
Решение от 21 юни 2011 г. по дело *Shimovolos/Русия*, № 30194/09
Решение от 14 февруари 2006 г. по дело *Turek/Словакия*, № 57986/00

Бази данни с регистри за съдимост

Решение от 17 декември 2009 г. по дело *B.B./Франция*, № 5335/06
Решение от 13 ноември 2012 г. по дело *M.M./Обединеното кралство*, № 24029/07

Бази с ДНК данни

Решение от 4 декември 2008 г. по дело *S. и Marper/Обединеното кралство*, № 30562/04 и 30566/04

GPS данни

Решение от 2 септември 2010 г. по дело *Uzun/Германия*, № 35623/05

Данни за здравословното състояние

Решение от 25 ноември 2008 г. по дело *Biriuk/Литва*, № 23373/03.
Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03
Решение от 10 октомври 2006 г. по дело *L.L./Франция*, № 7508/02
Решение от 2 юли 2002 г. по дело *M.S./Швеция*, № 34209/96
Решение от 2 юни 2009 г. по дело *Szuluk/Обединеното кралство*, № 36936/05
Решение от 25 февруари 1997 г. по дело *Z./Финландия*, № 22009/93

Самоличност

Решение от 27 април 2010 г. по дело *Ciubotaru/Молдова*, № 27138/04
Решение от 25 септември 2012 г. по дело *Godelli/Италия*, № 33783/09
Решение от 13 февруари 2003 г. по дело *Odièvre/Франция* [голям състав], № 42326/98

Информация, отнасяща се до професионални дейности

Решение от 6 декември 2012 г. по дело *Michaud/Франция*, № 12323/11
Решение от 16 декември 1992 г. по дело *Niemitz/Германия*, № 13710/88

Прихващане на комуникации

Решение от 16 февруари 2000 г. по дело *Amann/Швейцария* [голям състав], № 27798/95
Решение от 3 април 2007 г. по дело *Copland/Обединеното кралство*, № 62617/00
Решение от 3 юни 2003 г. по дело *Cotlet/Румъния*, № 38565/97
Решение от 24 април 1990 г. по дело *Kruslin/Франция*, № 11801/85
Решение от 24 август 1998 г. по дело *Lambert/Франция*, № 23618/94
Решение от 1 юли 2008 г. по дело *Liberty и други/Обединеното кралство*, № 58243/00
Решение от 26 април 1985 г. по дело *Malone/Обединеното кралство*, № 8691/79
Решение от 25 юни 1997 г. по дело *Halford/Обединеното кралство*, № 20605/92
Решение от 2 юни 2009 г. по дело *Szuluk/Обединеното кралство*, № 36936/05

Задължения на лицата, които носят отговорност

Решение от 17 декември 2009 г. по дело *B.B./Франция*, № 5335/06

Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03
Решение от 10 май 2011 г. по дело *Mosley/Обединеното кралство*, № 48009/08

Снимки

Решение от 11 януари 2005 г. по дело *Sciacca /Италия*, № 50774/99
Решение от 24 юни 2004 г. по дело *Von Hannover/Германия*, № 59320/00

Правото „да бъдеш забравен“

Решение от 6 юни 2006 г. по дело *Segerstedt-Wibergu други/Швеция*, № 62332/00

Право на възражение

Решение от 26 март 1987 г. по дело *Leander/Швеция*, № 9248/81
Решение от 10 май 2011 г. по дело *Mosley/Обединеното кралство*, № 48009/08
Решение от 2 юли 2002 г. по дело *M.S./Швеция*, № 34209/96
Решение от 4 май 2000 г. по дело *Rotaru/Румъния*, [голям състав], № 28341/95

Чувствителни категории данни

Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03
Решение от 6 декември 2012 г. по дело *Michaud/Франция*, № 12323/11
Решение от 4 декември 2008 г. по дело *S. и Marper/Обединеното кралство*, № 30562/04 и 30566/04

Надзор и правоприлагане (роля на различните участници, включително на органите за защита на данните)

Решение от 17 юли 2008 г. по дело *I./Финландия*, № 20511/03
Решение от 2 декември 2008 г. по дело *K.U./Финландия*, № 2872/02
Решение от 24 юни 2004 г. по дело *Von Hannover/Германия*, № 59320/00
Решение от 7 февруари 2012 г. по дело *Von Hannover/Германия (№ 2)* [голям състав], № 40660/08 и 60641/08

Методи за наблюдение

Решение от 5 ноември 2002 г. по дело *Allan/Обединеното кралство*, № 48539/99
Решение от 24 май 2011 г. по дело *Association "21 Décembre 1989" и други/Румъния,* № 33810/07 и 18817/08
Решение от 10 март 2009 г. по дело *Bykov/Русия* [голям състав], № 4378/02
Решение от 18 май 2010 г. по дело *Kennedy /Обединеното кралство*, № 26839/05
Решение от 6 септември 1978 г. по дело *Klass и други/Германия*, № 5029/71
Решение от 4 май 2000 г. по дело *Rotaru/Румъния*, [голям състав], № 28341/95
Решение от 22 октомври 2002 г. по дело *Taylor-Sabori/Обединеното кралство*, № 47114/99
Решение от 2 септември 2010 г. по дело *Uzun/Германия*, № 35623/05
Решение от 31 май 2005 г. по дело *Vetter/Франция*, № 59842/00

Видео наблюдение

Решение от 5 октомври 2010 г. по дело *Köpke /Германия*, № 420/07
Решение от 28 януари 2003 г. по дело *Peck/Обединеното кралство*, № 44647/98

Гласови образци

Решение от 25 септември 2001 г. по дело *P.G. и J.H./Обединеното кралство*, № 44787/98

Решение от 20 декември 2005 г. по дело *Wisse/Франция*, № 71611/01

Избрана съдебна практика на Съда на Европейския съюз

Съдебна практика, свързана с Директивата за защита на личните данни

Решение от 16 декември 2008 г. по дело *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy u Satamedia Oy*, C-73/07

[Понятие за „журналистическа дейност“ по смисъла на член 9 от Директивата за защита на личните данни]

Решение от 9 ноември 2010 г. по съединени дела *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen*, C-92/09 и C-93/09

[Пропорционалност на правното задължение да се публикуват лични данни относно бенефициентите по определени земеделски фондове на ЕС]

Решение от 6 ноември 2003 г. по дело *Bodil Lindqvist*, C-101/01

[Законност на публикуването на данни от частно лице относно личния живот на други лица в интернет]

Преюдициално запитване, отправено от *Audiencia Nacional* (Испания) на 9 март 2012 г. — *Google Spain, S.L., Google, Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González*, дело C-131/12, 25 май 2012 г., предстоящо решение

[Задължения на доставчиците на търсачки да се въздържат, по искане на физическо лице, от показване на лични данни в резултатите от търсенето]

Съд на ЕС, Решение от 30 май 2013 г. по дело *Европейска комисия/Кралство Швеция*, C-270/11

[Глоба за неприлагане на директива]

Решение от 29 януари 2008 г. по дело *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06

[Задължение на доставчиците на услуги за достъп до Интернет да разкрият на сдружение за защита на интелектуалната собственост самоличността на потребителите на програми за споделяне на файлове KaZaA]

Европейска комисия/Унгария, дело C-288/12: 8 април 2014 г.

[Законност на отстраняването от длъжност на националния надзорен орган за защита на данните]

C-291/12, Заключение на генералния адвокат от 13 юни 2013 г. по дело *Michael Schwarz/Stadt Bochum*

[Нарушение на първичното право на ЕС с Регламент (ЕО) 2252/2004, който предвижда съхраняването на дактилоскопични отпечатъци в паспортите]

Решение от 16 февруари 2012 г. по дело *SABAM/Netlog N.V.*, C-360/10

[Задължение на доставчиците на платформи за социални мрежи да предотвратяват незаконосъобразното използване на музикални и аудиовизуални произведения от мрежовите потребители]

Решение 20 май 2003 г. по съединени дела *Rechnungshof/Österreichischer Rundfunk и други и Neukomm и Lauermann/Österreichischer Rundfunk*, C-465/00, C-138/01 и C-139/01

[Пропорционалност на правното задължение да се публикуват лични данни относно заплатите на служители в определени категории, свързани с публичния сектор, институции]

Решение от 24 ноември 2011 г. по съединени дела *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) и Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, C-468/10 и C-469/10

[Правилно прилагане на член 7, буква е) от Директивата за защита на личните данни – „законните интереси на други лица“ – в националното законодателство]

Решение от 9 март 2010 г. по дело *Европейска комисия/Федерална република Германия*, C-518/07

[Независимост на национален надзорен орган]

Решение от 16 декември 2008 г. по дело *Huber/Bundesrepublik Deutschland*, C-524/06

[Законност на съхранението на данни за чужденците в статистически регистър]

Решение от 5 май 2011 г. по дело *Deutsche Telekom AG/Bundesrepublik Deutschland*, C-543/09
[Необходимост от подновено съгласие]

Решение от 7 май 2009 г. по дело *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, C-553/07
[Право на достъп на физическото лице]

Съединени дела C-293/12 и C-594/12, *Digital Rights Ирландия и Seitling и други*, 8 април 2014 г.
[Нарушаване на първичното право на ЕС от Директивата за запазване на лични данни]

Решение от 16 октомври 2012 г. по дело *Европейска комисия/Република Австрия*, C-614/10
[Независимост на националния надзорен орган]

Съдебна практика, свързана с Регламента относно защитата на данните при обработването им от институции на ЕС

Решение от 29 юни 2010 г. по дело *Европейска комисия/The Bavarian Lager Co. Ltd*, C-28/08 P
[Достъп до документи]

Решение от 6 март 2003 г. по дело *Interporc Im- und Export GmbH/Комисия на Европейските общности*, C-41/00 P
[Достъп до документи]

Решение от 15 юни 2010 г. по дело *Pachtitis/Европейска комисия и EPSO*, F-35/08
[Използването на лични данни в контекста на трудовите правоотношения в институциите на ЕС]

Решение на Съда на публичната служба от 5 юли 2011 г. по дело *V/Парламент*, F-46/09
[Използването на лични данни в контекста на трудовите правоотношения в институциите на ЕС]

Списък на дела

Практика на Съда на Европейските общности

Практика на Европейския съд по правата на човека

Практика на националните съдилища

Агенция за основните права на Европейския съюз
Съвет на Европа - Европейски съд по правата на човека

Наръчник по европейско право в областта на защитата на данните

2014 — 227 стр. — 14.8 × 21 см

ISBN 978-92-871-9950-8 (CE)
ISBN 978-92-9239-325-0 (FRA)
doi:10.2811/53167

Голяма част от информацията на Агенцията за основните права на Европейския съюз е налична в Интернет. Може да бъде потърсена на страницата на АОП- fra.europa.eu.

Повече информация за Съвета на Европа можете да получите чрез интернет, от hub.coe.int.

Допълнителна информация относно практиката на Европейския съд по правата на човека е налична на страницата на Съда: echr.coe.int. Порталът за търсене HUDOC осигурява достъп до съдебни и други решения на английски/френски език, преводи на други езици, резюмета по правни въпроси, прес-съобщения и друга информация относно работата на Съда.

КАК ДА СЕ СДОБИЕМ С ПУБЛИКАЦИИТЕ НА ЕС?

Безплатни публикации:
- един екземпляр:
  чрез EU Bookshop (http://bookshop.europa.eu);
- повече от един екземпляр или постери/карти:
  от представителствата на Европейския съюз (http://ec.europa.eu/represent_bg.htm);
  от делегациите в страни извън Европейския съюз (http://eeas.europa.eu/delegations/index_en.htm);
  като се свържете с услугата Europe Direct (http://europa.eu/europedirect/index_en.htm) се обадите на 00 800 6 7 8 9 10 11 (безплатен номер в ЕС) (*).

Платени публикации:
- чрез EU Bookshop (http://bookshop.europa.eu);

Платени абонаменти:
- чрез някой от търговските представители на Службата за публикации на Европейския съюз (http://publications.europa.eu/others/agents/index_bg.htm).

(*) информацията, както и повечето обаждания са безплатни (възможно е обажданията от мрежата на някои оператори, от обществени телефони или от хотели да бъдат таксувани).

Как да се сдобием с публикациите на Съвета на Европа

Издателството на Съвета на Европа публикува трудове от всички сфери на дейността на организацията, включително правата на човека, правни науки, здравеопазване, етика, социално дело, околна среда, образование, култура, спорт, младежта и архитектурното наследство. Книги и електронни издания от пълния каталог можете да поръчате онлайн (http://book.coe.int/).

Виртуална читалня дава възможност на потребителя да прегледа безплатно откъси от трудове с голямо значение, които току- що са били публикувани, както и пълния текст на някои официални документи.

Информация за Конвенцията на Съвета на Европа, както и пълния ѝ текст може да намерите на интернет страницата на Отдела по договорите: http://conventions.coe.int/.

10.2811/53167 TK-01-13-772-BG-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Бързото развитие на информационните и комуникационните технологии подчертава нарастващата необходимост от стабилна защита на личните данни — право, гарантирано както от актовете на Европейския съюз (ЕС), така и от тези на Съвета на Европа (СЕ). Технологичният напредък, например, разширява границите на наблюдението, прихващането на комуникации и съхранението на данни, като той поражда значителни предизвикателства по отношение на правото на защита на данните. Наръчникът е предназначен да запознае практикуващите юристи, които не са специализирали в областта на защитата на данните, с тази област на правото. Той предоставя преглед на приложимите правни рамки на ЕС и на Съвета на Европа. В него се обяснява ключова съдебна практика, като обобщено са представени основните решения на Европейския съд по правата на човека (ЕСПЧ) и на Съда на Европейския съюз (Съда на ЕС). В случаите, когато не съществува такава съдебна практика, в него са представени практически примери с хипотетични сценарии. Казано накратко, този наръчник има за цел да спомогне да се гарантира, че правото на защита на данните се отстоява с енергичност и решителност.

АГЕНЦИЯ ЗА ОСНОВНИ ПРАВА НА ЕВРОПЕЙСКИЯ СЪЮЗ
Schwarzenbergplatz 11 – 1040, гр. Виена - Австрия
Тел. +43 (1) 580 30-60 – Факс: +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

СЪВЕТ НА ЕВРОПА
ЕВРОПЕЙСКИ СЪД ПО ПРАВАТА НА ЧОВЕКА
67075 Старсбург Cedex - Франция
Тел. +33 (0) 3 88 41 20 00 - Факс: +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Служба за публикации
ISBN 978-92-871-9950-8 (CE)
ISBN 978-92-9239-325-0 (FRA)
ISBN 978-92-9239-325-0
9 789292 393250