FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

HELPING TO MAKE FUNDAMENTAL RIGHTS
A REALITY FOR EVERYONE IN THE EUROPEAN UNION

The General Data Protection Regulation – one year on

Civil society: awareness, opportunities and challenges

FRA Focus

The General Data Protection Regulation (GDPR) has applied across the European Union (EU) since 25 May 2018. One year on, this paper looks at how the new regulation has affected the daily work of civil society organisations (CSOs). Based on responses from over 100 CSOs engaged in a wide range of activities, it looks at how well these CSOs understand the EU data protection requirements, whether complying has been challenging, their interactions with supervisory authorities, their implementation efforts, and experiences with GDPR-based complaints. In so doing, the paper provides helpful insights for the European Commission's overall assessment of the GDPR's impact.

Contents

KEY FINDINGS

The General Data Protection Regulation (GDPR) has applied across the EU since 25 May 2018. One year on, the European Union Agency for Fundamental Rights (FRA) asked the civil society organisations (CSOs) that are part of the agency's Fundamental Rights Platform to answer a short online questionnaire about the impact of the GDPR on their daily work. This report is based on responses from 103 organisations. Respondents represent a wide range of CSOs, most of which do not work specifically in the field of privacy and data protection. This paper, which presents their replies, contributes to an overall assessment by the European Commission of the impact of the GDPR.

Understanding the GDPR

- The majority of respondents (66 %) indicated that they had either a fair or an expert understanding of EU data protection requirements.
- Almost half of the respondents (47 %) have a designated data protection officer.

Effort in complying with the GDPR

- The majority of respondents (77 %) indicated that their organisation faced challenges in implementing the GDPR.
- Seventeen per cent of respondents indicated that they did not find implementing the GDPR requirements' particularly challenging.
- The majority of respondents (89 %) indicated that complying with the GDPR required either a great deal of effort or some effort, while 8 % of respondents indicated that it required very little or no effort.
- Respondents' efforts mainly concerned:
  - the adoption or revision of privacy policies;
  - getting the consent of data subjects, in order to revise and/or delete mailing list subscribers.

Cooperation with supervisory authorities when implementing the GDPR

- Nearly half of respondents (48 %) indicated that their supervisory authority (formerly known as a "data protection authority") did not provide any assistance or advice with regard to the GDPR.
- The majority of respondents (72 %) indicated that their organisation did not have any direct contact with the supervisory authority of their country.
- The main reason that respondents contacted supervisory authorities was to seek clarity and advice on the GDPR's requirements. Some organisations contacted their national supervisory authority to ask specific questions related to the application of the GDPR, such as the designation of their data protection officer, how to deal with a complaint, and how to deal with a data breach.
  - Of those respondents who had contacted their supervisory authority, the majority had not faced any difficulties in their dealings with the authority. Half of them declared that they had received information on the GDPR from other sources.

Impact

- Thirty-seven per cent of responding organisations did not identify any impact of the GDPR on their work.
- Of those that indicated that the GDPR affects their work, many (37 %) declared that it makes their work "somewhat less" or "much less" efficient.
- The main challenges are linked with the legal basis for collecting and processing personal data (getting individuals' consent) and establishing which legal basis is appropriate for collecting and processing personal data.

GDPR implementation: individuals' access to personal data, privacy policies and data security

- The majority of the organisations that responded (73 %) have not received any access requests from individuals. Of those that have:
  - the majority of requests concern the erasure of personal data;
  - most requests were felt to be legitimate.
- The majority of respondents (73 %) have adopted a new privacy policy.
- Data security concerns:
  - Almost half of respondents (43 %) have no or few concerns about potential governmental surveillance of the personal data held by their organisation. However, around a quarter (27 %) indicated that they were very or extremely concerned.
  - A significant number of respondents (40 %) are concerned about unauthorised access (such as hacks).
  - Few organisations have found evidence of a data breach. Some data breaches were reported to the supervisory authority and some were deemed not to require a report to the supervisory authority by the organisation.

Complaints

- Few organisations declared that they had used the right, conferred by Article 80 of the GDPR, to file a complaint either on behalf of an individual or without any individual's mandate.
- Very few organisations indicated that they had filed a complaint on the basis of consumers' collective redress.
- One organisation indicated that a complaint based on the GDPR had been filed against it.

Introduction

Article 8 of the EU Charter of Fundamental Rights guarantees individuals' fundamental right to the protection of personal data. Article 8 also entails the key data protection principles associated with this fundamental right. The processing of personal data must be fair, for specified purposes, and based on either the consent of the person concerned or a legitimate basis laid down by law. Individuals must have the right to access their personal data and to have it rectified, and compliance with this right must be subject to control by an independent authority. The European Union Agency for Fundamental Rights (FRA), together with the Council of Europe and the European Data Protection Supervisor, published a handbook on European data protection law, which explores the application of this right in more detail.[1]

Since 25 May 2018, the General Data Protection Regulation[2] (GDPR) has applied across the 28 EU Member States. The regulation reforms and modernises data protection legislation in the EU. It provides a single set of data protection rules applicable in each EU Member State, thereby harmonising the implementation of the right to data protection across the EU. The GDPR benefits both businesses and individuals by establishing an environment of legal certainty.

The GDPR preserves and develops the core rights and principles set out in the 1995 Data Protection Directive. It also introduces new obligations for entities that process personal data. For instance, it requires the implementation of data protection by design and by default; it stipulates that a data protection officer must be appointed in certain circumstances; it establishes a new right to data portability and it also stipulates that entities must comply with the principle of accountability. In addition, the regulation introduces a number of procedural safeguards that oblige entities that deal with personal data to better inform individuals, to refrain from unnecessary or disproportionate use of personal data and to increase the security of stored data. These safeguards aim to better protect personal data with respect to their processing, but, nevertheless, may appear complex or burdensome for smaller and/or non-expert organisations, including some civil society organisations (CSOs).

CSOs play a crucial role in promoting and protecting fundamental rights.[3] CSOs often deal with personal data to effectively fulfil their mandate. For instance, they collect data on victims of alleged fundamental rights violations. Understanding how the GDPR has affected CSOs' work is a relevant part of any assessment of the GPDR's impact in its first year of application.

The European Commission's Directorate General for Justice and Consumers is conducting a major assessment of the GDPR's impact to mark the end of the regulation's first year of application. It sent a detailed questionnaire to a multi-stakeholder expert group, established in 2017 to support the application of the GDPR, which will assist the Commission in identifying potential challenges in the regulation's application.[4] The group includes academic experts, data controllers from the business sector and data protection supervisory authorities. A dedicated Eurobarometer survey will also provide important information on the impact of the GDPR.

FRA invited its Fundamental Rights Platform (FRP)[5] – composed of civil society actors – to complete a short online questionnaire about their understanding and experiences of the GDPR to support the Commission's assessment. The questionnaire addressed both the positive and the negative impacts of the GDPR on CSOs. It indicates how CSOs have addressed various issues in relation to the GDPR, although is not exhaustive.

This paper presents a brief, descriptive overview of the results of FRA's online questionnaire. It is divided into four sections. The first section assesses CSOs' general understanding of the GDPR. The second section discusses how CSOs cooperate with external stakeholders and, notably, with data protection supervisory authorities. The third section focuses on the application of the GDPR – including the replies given to individuals that have requested access to their own data and the methods used to ensure appropriate security of the data. The fourth section analyses how CSOs reply to complaints and deal with legal action.

1 See FRA *et al.* (2018).
2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016.
3 See FRA (2017).
4 European Commission (2017).
5 For more information on the FRP, including the list of participating organisations, see FRA's webpage on the FRP.

Overview of respondents

- **Number of respondents:** the analysis is based on 103 completed questionnaires, representing 14 % of all organisations registered in the FRP (752 organisations).
- **Types of organisations:** the majority of respondents represent non-governmental organisations (NGOs) dealing with human rights. Other organisations include universities; churches and religious, philosophical or non-confessional organisations; and other European and international expert bodies and organisations.
- **Profile of respondents:** 44 administrators with some responsibility for data protection; 18 chief executive officers (CEOs), chairs or directors; 16 legal experts; eight data protection officers (DPOs); and two board members. Other respondents (15) include communication experts, programme managers, advisers and team leaders.
- **Geographical scope of respondents:** respondents cover all 28 EU Member States. However, respondents are not equally spread across the Member States and do not represent the breadth of all organisations in the FRP.

1. Understanding and adapting to the GDPR

The majority of respondents (77 %) highlighted that their organisation faced challenges in complying with the GDPR. In addition, the majority of respondents (66 %) indicated that they have a fair or an expert understanding of EU data protection requirements.

The majority of respondents (65 %) indicated that the right to privacy and data protection were not the main areas of the work, advocacy or research undertaken by their organisation. This was the case for 32 % of the respondents.[6] However, the majority indicated that they had a fair or an expert understanding of EU data protection requirements (66 %). The other respondents indicated that they had a basic understanding of these requirements. No organisations indicated that they had no understanding of the new requirements.[7]

Organisations were asked to indicate whether or not they considered the application of the GDPR a challenge for their organisation.[8] The majority (77 %) indicated that their organisation faced challenges in this regard, while 20 % indicated that the GDPR did not present any specific challenges.

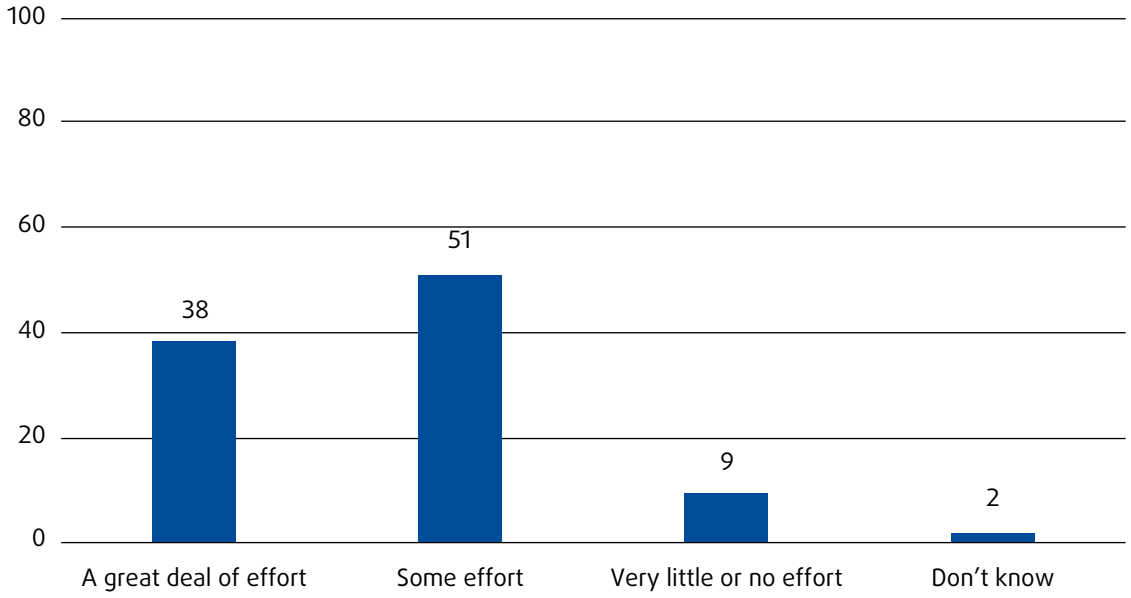
Respondents were asked whether or not the GDPR brought advantages to their organisation, such as the ability to better defend the interests of individuals or more clarity about the use of data.[9] Organisations were more divided in their responses to this question. Almost the same proportion of organisations saw opportunities in the GDPR (41 %) as the proportion that did not see any opportunities (44 %). Sixteen per cent of respondents did not know whether or not the GDPR had brought advantages to their organisations.

Respondents were asked to indicate whether or not their organisation had to make any additional efforts to comply with the GDPR, such as an increase in the time spent on data protection or in the human and/or financial resources used. A large proportion of respondents indicated that either a great deal of effort (38 %) or some effort (51 %) was required to comply with the GDPR (see Figure 1). Nine per cent of respondents indicated that very little or no effort was required. Respondents were invited to describe the nature of such efforts in their organisation, selecting one or several of the following:[10] "publishing or revising a privacy policy/statement"; "getting new consent, or revising or deleting mailing list subscribers"; "adopting or revising internal policies"; "reviewing or changing research procedures"; "implementing new IT systems, notably to reinforce their security"; "offering data protection training"; or "other".

6 See Annex 2, question 2.
7 See Annex 2, question 4.
8 See Annex 2, question 5.
9 See Annex 2, question 6.
10 See Annex 2, question 8.

The changes that were undertaken by organisations that indicated that either a great deal of effort or some effort was required to comply with the GDPR mainly concerned the publication or revision of privacy policies or statements, in relation to either external data subjects, through their mailing lists (74 %), or the adoption or revision of internal policies (73 %). Sixty per cent of these organisations indicated that most of their effort related to getting consent from data subjects, in order to revise and/or delete mailing list subscribers accordingly. Some organisations modified their working methods: 30 % implemented new IT systems to cope with the GDPR's requirements, while 24 % reviewed or amended their research procedures. Interestingly, 40 % of the organisations that indicated that either a great deal of effort or some effort was required to comply with the GDPR had provided specific training on data protection.

Figure 1: Scope of efforts required to comply with GDPR requirements (%)[a,b]



Notes: [a] *Of all respondents (n = 103).*
[b] *Question7: 'Has complying with the GDPR required efforts from your organisation, such as increased time being spent on data protection requirements, more human and/or financial resources being used for compliance?' (Options as listed in the figure.)*
Source: *FRA, 2019*

Specific concerns

When invited to add any further remarks in relation to the issues covered by this survey, several organisations indicated that smaller CSOs are more likely to lack awareness or understanding of, or fail to implement, GDPR requirements because of a lack of adequate resources. The GDPR's principles are "cumbersome", "complex" and "costly" for these organisations. The main concern lies in the likelihood that they could miss or misinterpret important legal requirements as a result of not being able to dedicate either human or financial resources to assessing the new data protection requirements properly. Several organisations referred to their need to receive information tailored to the specificities and needs of civil society.

2. Getting appropriate advice and cooperating with supervisory authorities

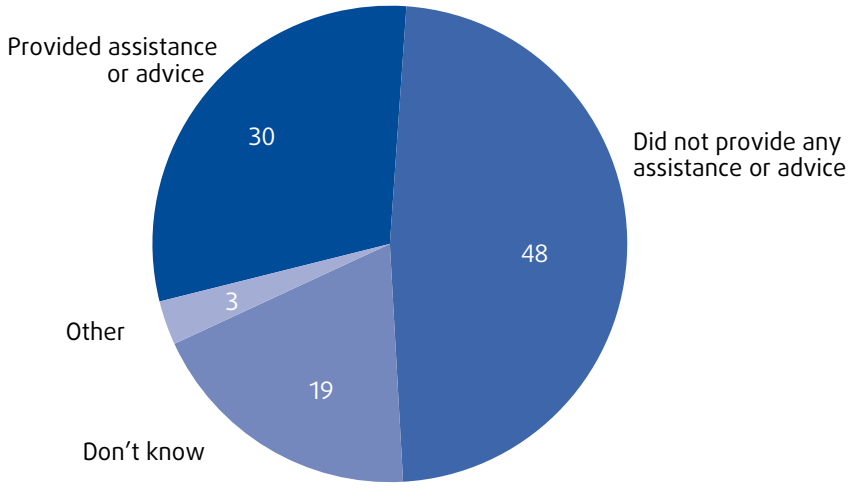
The majority of respondents (67 %) indicated that either there was a lack of support from or they were unaware of any assistance provided by the Member State supervisory authority responsible for data protection. This high proportion indicates a lack of communication between supervisory authorities and CSOs. Several respondents indicated that their organisations had to turn to private companies for assistance.

The GDPR has reinforced and widened the scope of the mandate of data protection authorities, referred to as "supervisory authorities" in the GDPR and throughout this paper. Novelties include the tasks to:

- "promote public awareness and understanding of the risks, rules, safeguards and rights in relation to data processing";
- "advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing";
- "promote the awareness of controllers and processors of their obligations under this Regulation";
- "provide information to any data subject concerning the exercise of their rights under this Regulation".[11]

The GDPR recognises the essential role of national data protection supervisory authorities in ensuring the promotion and understanding of the GDPR's requirements, for both businesses and individuals. The increase in the number of complaints received, as well as the increase in the financial and human resources attributed to supervisory authorities, reflects this extension of the supervisory authorities' powers.[12] However, many respondents (48 %) indicated that, to their knowledge, the relevant supervisory authority did not provide any assistance or advice to their organisation (for example in the form of a leaflet, online information, a helpline or training).[13] Nineteen per cent indicated that they did not know whether or not their national supervisory authority provided any assistance or advice (see Figure 2).

Figure 2: Assistance and advice provided by supervisory authorities to organisations on the application of the GDPR (%)[a,b]



Notes: [a] *Of all respondents (n = 103).*
[b] *Question 9: 'Has the Data Protection Authority in your country provided assistance or advice to your organisation about the application of the GDPR (for example in the form of a leaflet, online information, a helpline or training)?' (Options as listed in the figure.)*
Source: *FRA, 2019*

11 General Data Protection Regulation, Art. 57.
12 EDPB (2019).
13 See Annex 2, question 9.

A few organisations further indicated, in response to an open question, that, while their national supervisory authority did provide some information on its website, such information was either "incomplete" or "not particularly helpful". Of the 30 % of organisations that indicated that they had benefited from information from their supervisory authority, the main source of assistance or advice[14] was online or web-based information. Some organisations indicated that they had been provided with face-to-face support (such as training sessions or meetings).

The majority of respondents (72 %) indicated that their organisation had not been in contact with the supervisory authority in their country, and 9 % did not know whether or not such exchanges had taken place.[15] Of those organisations that had been in contact with their supervisory authorities, 70 % indicated that the reason for such contact was to obtain further information on their organisation's compliance with the GDPR. Some organisations contacted their national supervisory authority to ask specific questions related to the application of the GDPR. Some questions related to the designation of their data protection officer, some related to a complaint and some related to a data breach. Organisations that had established direct contact with their national supervisory authorities were mainly engaged in advocacy, conducting campaigns, and education and awareness raising.

A large majority (85 %) of the organisations that had contacted their national supervisory authority indicated that they had not experienced any difficulties in their dealings with the authority. The organisations that did face difficulties (15 %) indicated that these were linked to either a long delay in receiving guidance or a lack of assistance that was specific to the needs of their organisation.[16]

Respondents were asked whether or not they had received advice on the GDPR from other experts or bodies.[17] Half of the respondents (52 %) declared that they had received information from other sources about how their organisation should operate to comply with the GDPR:

- 24 % from private companies that charge fees;
- 16 % from a government office;
- 60 % from another organisation.

14 See Annex 2, question 10.
15 See Annex 2, questions 11 and 12.
16 See Annex 2, questions 13 and 14
17 See Annex 2, questions 20 and 21.

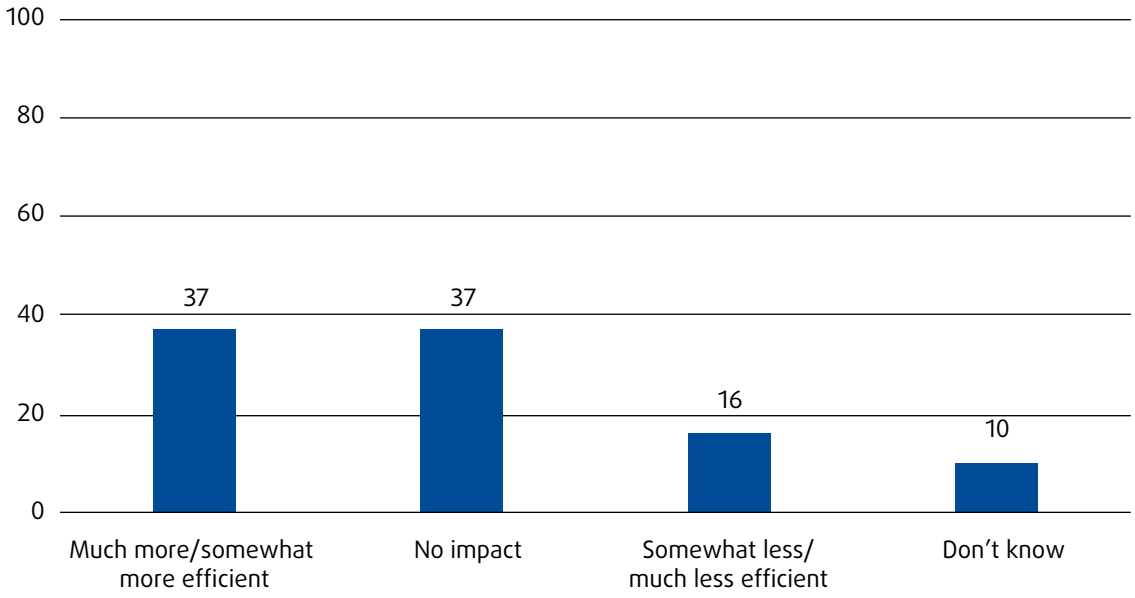
3. Applying the GDPR

3.1 General impact of GDPR on daily work of civil society organisations

Seventeen per cent of respondents indicated that implementing the GDPR's requirements did not affect the efficiency of their organisation. Many respondents (37 %) indicated that it did not have any impact on most of their day-to-day activities. This shows that, for a number of CSOs, complying with the GDPR has not been problematic.

Many respondents indicated that the GDPR did not have any impact on the efficiency of their day-to-day work (37 %), as illustrated in Figure 3.[18] Another 37 % of respondents indicated that the GDPR had made their work somewhat less or much less efficient, while 16 % of respondents declared that the GDPR had made their work somewhat more or much more efficient. The main activities of the organisations that declared that the GDPR had a negative impact are related to research and data collection, and finance.[19] The majority of organisations that declared that the adoption of the GDPR had made their work somewhat less efficient or much less efficient operate in the field of access to justice; economic and social rights; poverty eradication; education; or immigration, asylum and return, and integration.[20]

Figure 3: Evaluation of the general impact of the GDPR on the efficiency of organisations' day-to-day work (%)[a,b]



Notes: [a] *Of all respondents (n = 103).*
[b] *Question 15: 'Overall, how would you describe the impact of GDPR on the efficiency of your organisation's day-to-day work?' (Options as listed in the figure.)*
Source: *FRA, 2019*

18 See Annex 2, question 15.
19 See Annex 2, question 15 combined with question 38d.
20 See Annex 2, question 15 combined with question 38e.

Specific concerns

Some organisations reported cases in which official bodies had denied them access to sensitive information (such as data on ethnic origin) on the basis of the GDPR. This is particularly concerning, as it could prevent organisations that work on, for instance, the prevention of discrimination or victim support from being effective. One organisation indicated that they had to provide information and analysis to statutory service providers, which, as the organisation understands it, were using the GDPR in order not to provide the NGO with data on ethnicity. Several of the respondents, when invited to add any further remarks in relation to the issues covered by this survey, highlighted concerns that some governmental bodies may misuse the GDPR against CSOs. Concerns include potential threats to CSOs from state actors, the abuse of fines, strict interpretations of GDPR requirements to weaken CSOs' effectiveness and limiting the action of small NGOs, in particular those that perform advocacy or watchdog activities.

For further information on CSOs' concerns, see FRA (2017), Challenges facing civil society organisations working on human rights in the EU.

CSOs were asked to indicate which specific aspect of the GDPR they found particularly difficult to implement, by selecting one or several of the following answers:[21]

- Determining which legal basis to use to legitimise your collection/processing of personal data (Article 6 GDPR)
- Getting consent from individuals (Article 7(4) GDPR)
- Providing individuals with access to their personal data
- I have not found the GDPR requirements particularly challenging
- Other, please specify.

Of all respondents, 55 % identified getting individuals' consent as the main challenge, while 45 % declared that they had had difficulties in establishing the appropriate legal basis for collecting and processing personal data. Finally, 21 % of the respondents found the obligation to provide individuals with access to their data challenging.

Some organisations specified and elaborated on the challenges they face. Notably, they expressed concerns regarding the specific expectations, legal requirements and potential consequences for CSOs. Such organisations may have limited financial and human resources (as many CSOs rely on volunteers), and rely on access to the personal, often sensitive, data of individuals to support them in the protection of their rights.

On the other hand, 17 % of respondents indicated that they did not find complying with the GDPR particularly challenging.[22]

Likewise, many respondents indicated that the GDPR had had no impact on most of their day-to-day activities when asked whether or not the GDPR had had an impact on specific aspects of their work[23] (including contact with external supporters/members, partners or stakeholders, use of communication tools and use of social media).

Of those respondents who indicated that the GDPR had had some impact, the proportion who perceived it as having had a negative effect on their daily work generally outweighed the proportion who perceived a positive impact, as illustrated in Figure 4.

Thirty-six per cent of respondents indicated that the GDPR had had a negative impact on the use of traditional communication tools, such as telephone, post and email. Of these respondents, most work in victim support, gender equality and social integration.

It is interesting to note that most organisations that listed advocacy as one of their main activities believed that the GDPR had either no impact (56 %) or a positive impact (13 %) on their contact with external supporters or members, and either no impact (67 %) or a positive impact (9 %) on their contact with external stakeholders.

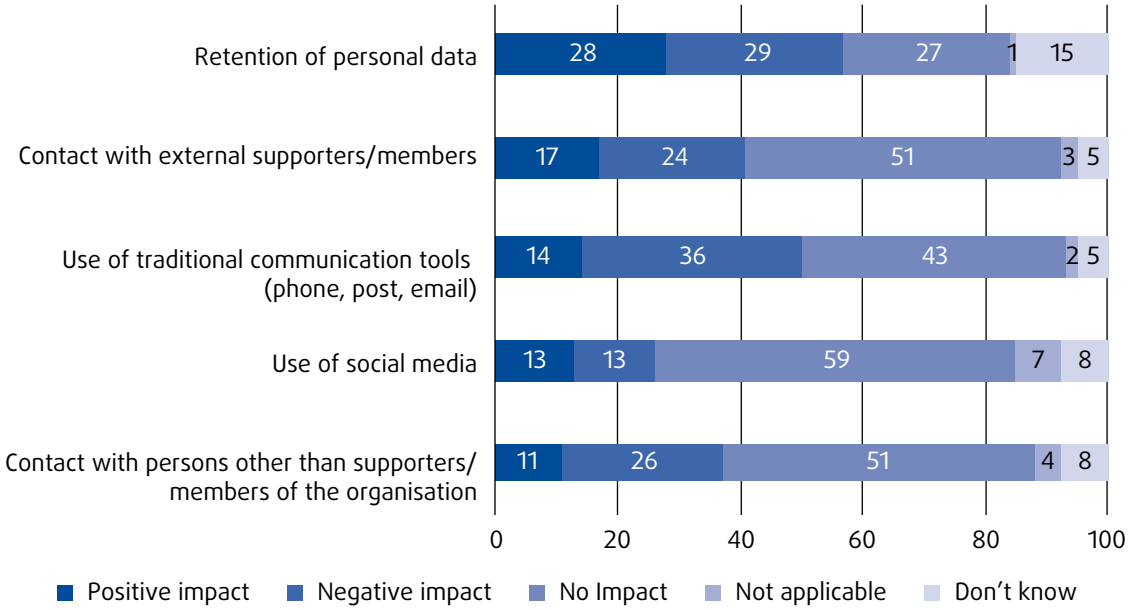
Retention of personal data seems to be the most ambiguous issue with regard to the impact of the GDPR on day-to-day activities. Over a quarter of respondents (28 %) identified the GDPR as being positive in relation to retention of personal data, while similar proportions of respondents identified either a negative (29 %) or no (27 %) impact in relation to this. Fifteen per cent had no opinion about the issue. Smaller proportions (from 11 % to 17 %) of respondents indicated that the GDPR had had a positive impact in relation to other issues, such as contact with supporters or the use of different communication tools.

21 See Annex 2, question 16.

22 See Annex 2, question 16.

23 See Annex 2, question 17.

Figure 4: Impacts of the GDPR on various day-to-day activities of civil society organisations (%)[a,b,c]



Notes: [a] *Of all respondents (n = 103).*
[b] *Question 17: 'Please clarify whether the GDPR has had any positive or negative impact on how your organisation does any of the following.' (Options as listed in the figure.)*
[c] *Sorted in order of proportion indicating a "positive impact".*
Source: *FRA, 2019*

3.2 Responding to individuals' requests

Most organisations did not receive any requests from data subjects for access to their data. Of those that did, the majority concerned requests for the erasure of personal data. Almost none of these requests was deemed to be manifestly unfounded or excessive.

The GDPR provides individuals with the right to access their personal data, among other rights. The regulation clarifies that data subjects may ask any organisation that processes their personal data to provide them with access to their data, modify their data or erase their data.

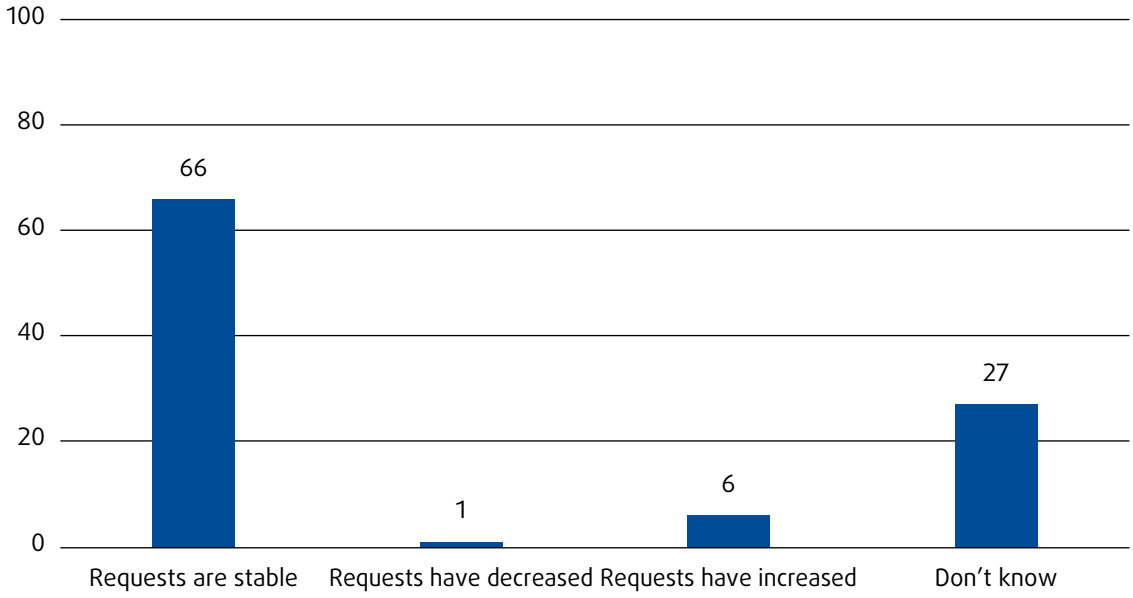
The majority of respondents' organisations (73 %) had not received any such requests from individuals between May 2018 and March 2019.[24] Organisations that had received such requests (26 %) were asked to give the reason(s) for these requests.[25] Most of the requests concerned the erasure of personal data (59 % of all requests), followed by requests from data subjects for access to their data (33 % of all requests) and for their personal data to be modified (30 % of all requests). In a few cases, the organisation received a request for a meaningful explanation and human intervention in an automated decision-making process.

The large majority of the requests received were not deemed manifestly unfounded or excessive (81 %) by respondents. Of the requests that were assessed as manifestly unfounded or excessive, half of these were believed to be malicious, made either to cause inconvenience to the organisation or to gain access to confidential information.

In terms of the impact of the GDPR on CSOs' workloads,[26] the majority of organisations (66 %) indicated that the number of requests received before and the number received after the date of application of the GDPR (25 May 2018) were similar (Figure 5). A significant number of organisations declared that they did not have sufficient information to ascertain whether the number of requests had decreased or increased (27 %). However, of those respondents who did have this information, only 6 % indicated that, to their knowledge, the number of requests had increased since the entry into force of the GDPR.

24 See Annex 2, question 25.
25 See Annex 2, question 26.
26 See Annex 2, question 25.

Figure 5: Changes in the number of requests for access to personal data since May 2018 (%)[a,b]



Notes: [a] *Of all respondents (n = 103).*
[b] *Question 29: 'Since May 2018, have you received requests from individuals to access, modify and/or delete their personal data?' (Options as listed in the figure.)*
Source: *FRA, 2019*

3.3 Ensuring appropriate security

Forty per cent of organisations declared that they are concerned by potential unauthorised access to personal data, and 27 % indicated that potential surveillance by governmental bodies is a concern. In addition, 5 % of respondents declared that their organisation does not have any data security policy. Although this percentage is small, it does give rise to concerns about organisations' awareness of their need to comply with the new regulation.

The security of personal data is very important for most CSOs, which as part of their daily activities may have to process very sensitive and/or confidential information. Of the organisations consulted, 10 % declared that they had suffered a data breach since May 2018. For two thirds of these, a report to the supervisory authority by the organisation was not deemed necessary.

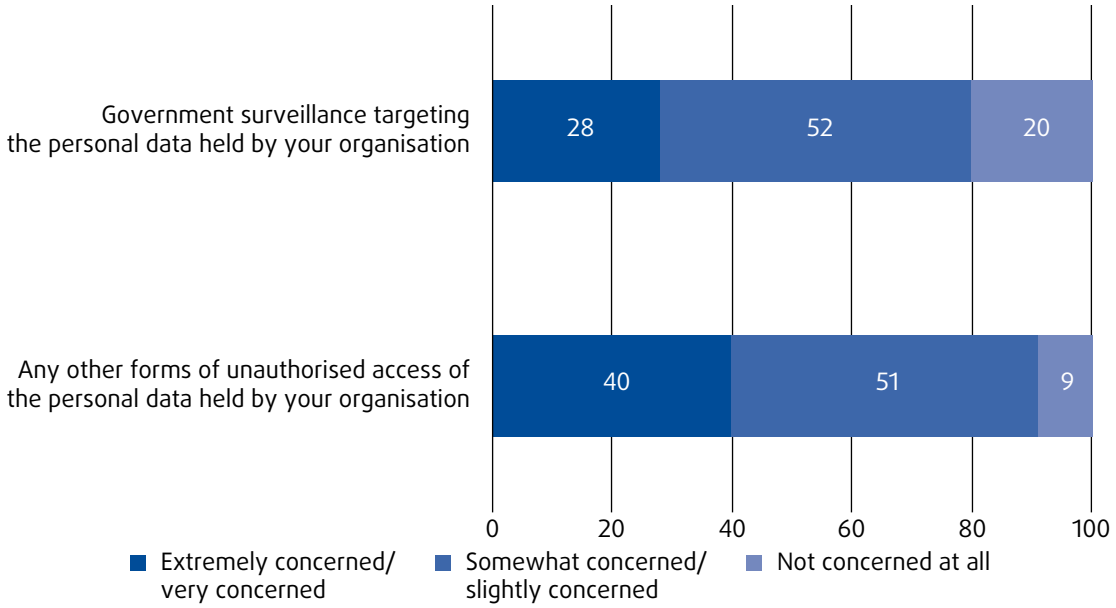
Still, most organisations (40 %) declared being concerned ("very concerned" or "extremely concerned") or slightly concerned (51 %) by potential unauthorised access to personal data. Concerns regarding potential surveillance by governmental bodies (see Figure 6) are noteworthy, as 28 % indicated that they are either very or extremely concerned about this.[27]

The majority of respondents (75 %) have adopted a new data protection policy since the date of application of the GDPR,[28] while 18 % still use the same data protection policy as that used before May 2018.

Some respondents felt that they needed to use technological measures to effectively manage security threats. Of the respondents who declared that they were somewhat to extremely concerned by any forms of unauthorised access other than government surveillance, 64 % had installed a new IT system within their organisation. Half of the organisations that had government surveillance concerns had set up a new IT system.[29]

27 See Annex 2, question 23.
28 See Annex 2, question 22.
29 See Annex 2, question 22 combined with question 8.

Figure 6: Civil society concerns in relation to unauthorised access and governments' surveillance of the personal data they hold (%)[a,b]



Notes: [a] *Of all respondents (n = 103).*
[b] *Question 23: 'On a scale from 0 to 5 (0 being not concerned at all, and 5 being extremely concerned), how concerned are you about (options as listed in the figure)?'*
Source: *FRA, 2019*

4. Facing complaints and legal actions

Few organisations declared that they had filed a complaint related to data protection. Some of these complaints were filed using the right conferred by Article 80 of the GDPR to file a complaint either on behalf of an individual or without any individual's mandate. Some were filed on the basis of consumers' collective redress.

The GDPR gives CSOs that are active in the field of protecting the rights and freedoms of data subjects the ability to lodge a complaint on behalf of an individual or independently.[30]

CSOs that are particularly active in the field of protecting personal data and respect for private life quickly made use of the powers conferred on them following the entry into force of the GDPR and filed several complaints. For example, the Austrian association "None Of Your Business" (NOYB) and the French association La Quadrature du Net (LQDN) filed collective complaints with the French supervisory authority, Commission Nationale de l'Informatique et des Libertés (CNIL), against Google, notably on the absence of an appropriate legal basis for collecting and processing personal data. The French association was mandated by more than 12,000 individuals to file this complaint.[31] On 21 January 2019, the French supervisory authority published its decision, and imposed on Google a financial penalty of € 50 million in accordance with the GDPR.[32]

Only very few organisations (three organisations) indicated that they had been mandated by an individual to file a data protection complaint (mainly with a supervisory authority) according to FRA's consultation with CSOs. Four organisations indicated that they had filed a complaint without being mandated by an individual (three on the basis of data protection legal requirements and one on the basis of consumers' collective redress). Of these, two were filed with a supervisory authority and two with a national court. Finally, one respondent indicated that a complaint based on the GDPR had been filed against their own organisation.[33]

It is interesting to note, however, that not all respondents who had lodged a complaint about a potential violation of GDPR requirements indicated that data protection was their main area of

30 GDPR, Art. 80.

31 France, La Quadrature du Net (2018).
32 France, CNIL (2019).
33 See Annex 2, questions 30 to 36.

work.[34] Data protection and privacy rights are the main area of work of:

1. only two of the organisations that lodged a complaint independently of any individual's complaint;

2. only one of the three organisations that lodged a complaint because of an individual's mandate to do.

This shows that, since the adoption of the GDPR, the awareness of data protection principles has increased outside specialist organisations, which in itself is a benefit of the GDPR.

34 See Annex 2, questions 30 and 32 combined with question 2.

References

Commission Nationale de l'Informatique et des Libertés (CNIL) (2019), *Délibération de la formation restreinte No. SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC*, SAN-2019-001, 21 January 2019.

European Data Protection Board (EDPB) (2019), *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities*,Brussels, 26 February 2019.

European Commission (2017), *Multistakeholder expert group to support the application of Regulation (EU) 2016/679*, E03537.

FRA (European Union Agency for Fundamental Rights) (2017), *Challenges facing civil society organisations working on human rights in the EU,* Luxembourg, Publications Office of the European Union (Publications Office).

FRA, European Court of Human Rights (ECtHR), Council of Europe (CoE) and European Data Protection Supervisor (EDPS) (2018), *Handbook on European data protection law – 2018 edition*, Luxembourg, Publications Office.

La Quadrature du Net, *Dépôt des plaintes collectives contre les GAFAM!*, 28 May 2018.

Annex 1 – Methodology and profile of respondents

Methodology

To collect information about the impact of the GDPR on civil society, FRA consulted its FRP,[35] which is composed of civil society actors in the field of fundamental rights at local, national, European and international levels. The FRP comprises largely non-governmental organisations (NGOs) dealing with human rights, but also trade unions and employers' organisations; relevant social and professional organisations; churches, religious, philosophical and non-confessional organisations; universities and other European and international expert bodies and organisations.

On 5 March 2019, FRA sent an online questionnaire to the FRP consisting of a series of questions (see Annex 2) around the following themes: the general understanding of the GDPR; cooperation with supervisory authorities; the application of the GDPR; data security and surveillance; requests from individuals; and complaints and legal actions.[36] The questionnaire included 10 open questions aimed at clarifying a reply, and one final open question.[37] The questionnaire was initially available for completion until 19 March, later extended until 24 March. FRA received 189 replies: 103 respondents fully completed the questionnaire and 86 questionnaires were incomplete. For the purpose of this report, only complete questionnaires were included in the analysis. Therefore, the findings illustrated below are based on a total number of 103 cases. This questionnaire, therefore, provides a snapshot of reactions from a specific group, and should not be understood as providing trends applying to all CSOs across the EU.

Profile of the responding organisations

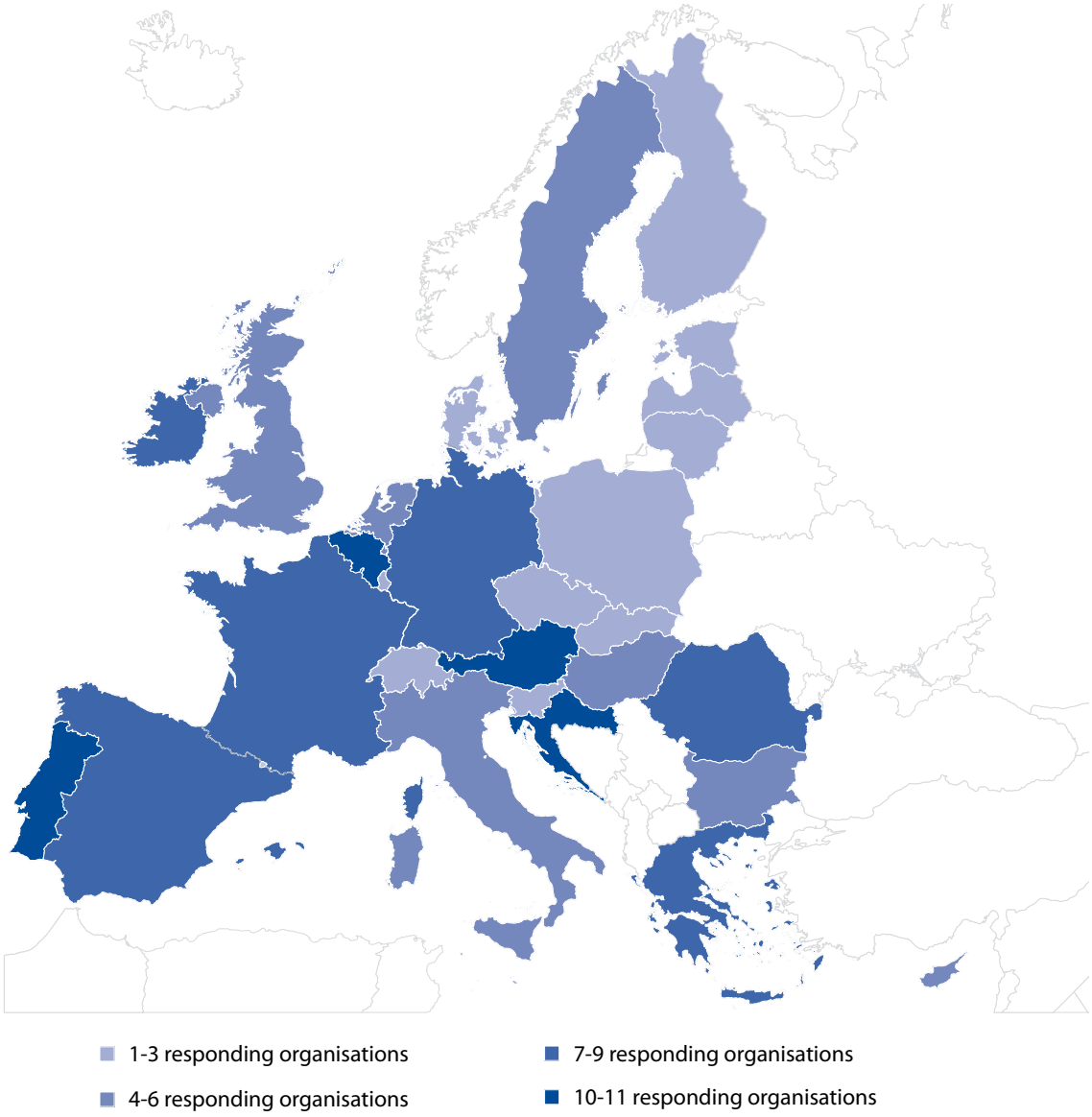
FRA encouraged the FRP organisations to invite their data protection officer (DPO), a legal expert or an administrator with some responsibility for data protection within their organisation to fill in the questionnaire. The questionnaire was completed by an administrator with some responsibility for data protection in 42 % of cases. Nineteen per cent of questionnaires were completed by the director, CEO, chair or board member of the organisation, and 15 % were completed by be a legal expert. While 47 % of responding organisations indicated that they have a data protection officer, only 7 % of those that filled in the questionnaire indicated that they fulfil the role of data protection officer. Other persons completing the questionnaire included communication experts (such as the spokesperson of the organisation), project or programme managers, and advisers and team leaders (17 %). The number of incomplete questionnaires could be explained by the fact that non-specialist respondents were unable to answer some specific questions.

The predominance of NGOs in the FRP was reflected in the types of organisations that replied to the questionnaire. Of the 103 respondents who clarified the status of their organisation, 88 described their organisations as NGOs, four as social and professional organisations, three as faith-based, religious, philosophical or non-confessional organisations, and two as universities or other European/international expert bodies or organisations.

Respondents were asked to clarify in which Member States they mainly worked or were based. All EU Member States were represented by at least one organisation (in the case of Czechia, Luxembourg, Malta and Slovakia) and some by up to 11 organisations (in the case of Austria, Belgium and Portugal), ensuring that the questionnaires covered all EU Member States. Thirty-two organisations indicated that most of their work encompasses all EU Member States (see Figure 7). Finally, a large majority of organisations have 16 or fewer employees (70 organisations), 21 organisations have between 16 and 100 employees and 11 have more than 101 employees.

35 For more information on the FRP, including the list of participating organisations, see FRA's webpage on the Fundamental Rights Platform.
36 See the full questionnaire in Annex 2.
37 See Annex 2, question 37.

Figure 7: Geographical coverage of responding organisations[a,b]



Notes: [a] *Out of all respondents (n=103).*
[b] *Question 38b: 'In which country does your organisation mainly work (or is based in)? Or do you work at the EU level – that is, your work having relevance for all EU Member States?' (multiple choices)*
Source: *FRA, 2019*

The 103 organisations were asked to indicate their main areas of engagement (respondents could select several from a list of options). Most work in education and awareness raising (67 organisations); advocacy (61 organisations); campaigning (33 organisations); the representation of victims, including victim support and counselling (31 organisations); and service provision such as social integration, social services, health projects and refugee support (30 organisations). Nineteen indicated that research and data collection is one of their main areas of engagement.

Finally, organisations were also asked to clarify their main fields of operation. Most indicated that they work on fundamental rights issues as a whole (45 organisations). The respondents who indicated either one or several fields of operation specialised in the following sectors: access to justice, including victims of crime (29 organisations); education (29 organisations); immigration, asylum and return, integration (29 organisations); and economic and social rights (24 organisations). Eight organisations indicated that their main field of operation was the information society, privacy and data protection.

Annex 2 – FRP questionnaire on the implementation of the GDPR

1. Please clarify your role in the organisation. Are you:

- A Data Protection Officer
- A legal expert
- An administrator with some responsibility for data protection
- Other: _____

General questions

2. Are data protection and the right to privacy main areas of work/advocacy/research for your organisation?

- Yes
- No
- Don't know

3. Has your organisation designated a "Data Protection Officer" (DPO)?

- Yes
- No
- Don't know

4. How would you rate your organisation's understanding of the new EU data protection requirements under the General Data Protection Regulation (GDPR)?

- No understanding of the new requirements
- Basic understanding – need the assistance of a data protection expert to understand the full extent of the new requirements
- Fair understanding – only need to check exact requirements depending on specific requests
- Expert understanding

5. Generally speaking, has your organisation experienced any **challenges** (such as increased administration, new rules difficult to understand, lack of resources, etc.) because of the new EU data protection rules since May 2018?

- Yes
- No
- Don't know

6. Generally speaking, has your organisation seen any **advantages** as a result of the new EU data protection rules since May 2018 (such as being able to defend better the interests of individuals, clarity about the use of data, etc.)?

- Yes
- No
- Don't know

7. Has complying with the GDPR required efforts from your organisation, such as increased time being spent on data protection requirements, more human and/or financial resources being used for compliance?

- A great deal of effort
- Some effort
- Very little or no effort
- Don't know

8. Have these **efforts** included one or more of the following (please select all that apply):

- Publishing or revising a privacy policy/statement
- In relation to your mailing list(s): getting new consent, or revising or deleting your mailing list subscribers
- Adopting or revising internal policies
- Reviewing or changing research procedures
- Implementing new IT systems, notably to reinforce their security
- Offering data protection training
- Other, please specify: _____

Cooperation with Data Protection Authorities

9. Has the Data Protection Authority in your country provided assistance or advice to your organisation about application of the GDPR (for example in the form of a leaflet, online information, a helpline or training)?

Please choose only one of the following:

- Yes
- No
- Don't know
- Other, please specify

10. How was the assistance provided?

- Leaflet and/or other printed material
- Online/web-based information
- A helpline
- Some form of training was offered
- Other, please specify:_____

11. On behalf of the organisation where you work, have you (or has your organisation) been in contact with the Data Protection Authority in your Member State concerning the new GDPR?

- Yes
- No
- Don't know

12. Why have you (or has your organisation) been in contact with the Data Protection Authority?

- Based on an individual's complaint
- To obtain further information on your organisation's compliance with the GDPR
- Other, please specify:_____

13. Did you experience any **difficulty** in your dealings with the Data Protection Authority?

- Yes
- No
- Don't know

14. Please specify the difficulties you experienced when dealing with the Data Protection Authority. Please select all that apply.

- Received no reply
- Long delay in providing guidance or advice
- Long delay in following up on a complaint
- Inadequate reply
- Other, please specify: _____
- Don't know

Applying the GDPR

15. Overall, how would you describe the impact of GDPR on the efficiency of your organisation's day-to-day work? The GDPR makes your work:

- Much less efficient
- Somewhat less efficient
- No impact
- Somewhat more efficient
- Much more efficient
- Don't know

16. Could you specify what are/were the GDPR requirements you found particularly **challenging**, if any, following the entry into force of the new regulation? Please select all that apply.

- Determining which legal basis to use to legitimate your collection/processing of personal data (Article 6 GDPR)
- Getting consent from individuals (Article 7(4) GDPR)
- Providing individuals with access to their personal data
- I have not found the GDPR requirements particularly challenging
- Other, please specify: _____

17. Please clarify whether the GDPR has had any positive or negative impact on how your organisation does any of the following (select all that apply).

	Yes – positive impact since introduction of GDPR	Yes – negative impact since introduction of GDPR	No impact	Not applicable	Don't know
Contact with external supporters/members					
Contact with persons other than supporters/members of your organisation					
Use of traditional communication tools (phone, post, email)					
Use of social media					
Retention of personal data					

18. You indicated that GDPR has had some **positive** impact on how your organisation works – please can you briefly say why this is?

19. You indicated that GDPR has had some **negative** impact on how your organisation works – please can you briefly say why this is?

20. Apart from your national data protection authority, has your organisation received advice or information from any other source about the way your organisation operates to comply with GDPR?

- Yes
- No
- Don't know

21. Was this other source:

- A private company charging fees
- A government office
- Another organisation
- Don't know

Data security and surveillance

22. Has your organisation adopted a new data protection policy following the adoption of the GDPR?

- Yes
- No – we use the same data protection policy as before

- No – we do not have a data protection policy
- Don't know

23. On a scale from 0 to 5 (0 being not concerned at all, and 5 being extremely concerned), how concerned are you about:

– government surveillance targeting the personal data your organisations holds

- 0 – Not concerned at all
- 1
- 2
- 3
- 4
- 5 – Extremely concerned

– any other forms of unauthorised access (such as hacking etc.) of the personal data your organisation holds

- 0 – Not concerned at all
- 1
- 2
- 3
- 4
- 5 – Extremely concerned

24. A data breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Art. 33 GDPR). For your organisation, have you reported any breach of personal data to the national data protection authority since May 2018?

- Yes
- No – there was no data breach
- No – there were data breaches, but that did not require to be reported to the Data Protection Authority
- Don't know
- Do not understand the question

Requests from individuals

25. Since May 2018, have you received requests from individuals to access, modify and/or delete their personal data?

- Yes
- No
- Don't know

- Don't understand the question

26. In relation to what have you received requests? Please select all that apply.

- In relation to the access to personal data
- In relation to the rectification of personal data
- In relation to the erasure of personal data
- Requests for meaningful explanation and human intervention in automated decision making
- Other, please specify:_____

27. Have you found some of such requests received to be manifestly unfounded or excessive?

- Yes
- No
- Don't know

28. Did you consider any of such requests to be maliciously or abusively made in order to inconvenience your organisation or to access information that should otherwise be confidential?

- Yes
- No
- Don't know

29. Have you noticed a change in the number of these requests since May 2018?

- Requests have increased
- Requests are stable
- Requests have decreased
- Don't know

Complaints and legal actions

30. Since May 2018, has somebody (one or more individuals) mandated your organisation to file a data protection complaint on their behalf?

- Yes
- No, nobody has asked us to do so
- No, our organisation doesn't take up complaints on people's behalf
- Do not understand the question

31. Did your organisation file such a complaint with:

- a Data Protection Authority
- a Court

- Other: _____
- Don't know

32. Has your organisation filed a complaint on its own initiative (without being requested to do so by an individual)?

- Yes
- No
- Don't know
- Don't understand the question

33. On what was the filed complaint based on?

- Based on Art. 80(2) GDPR
- Based on consumers' collective redress
- Based on specific provisions not related to consumers' collective redress

34. Please specify the specific provisions not related to consumers' collective redress.

Please write your answer here:_____

35. Did your organisation file such a complaint with:

- a Data Protection Authority
- a Court
- Other: _____
- Don't know

36. Are you aware of any complaints based on the GDPR that have been filed against your organisation?

- Yes, please specify:_____
- No
- Don't know

Any other observations

37. Please provide any other remarks you would like to share with us in relation to the issues covered by this survey

Information about your organisation

38a. On which level is your organisation active? (you can choose more than one response):

- Local/regional
- National
- EU/international

38b. In which country does your organisation mainly work (or is based in)? Or do you work at the EU level – that is, your work having relevance for all EU Member States?

38c. Which of the following best describes your organisation (categories as per FRA Founding Regulation, Art. 10) (only one answer possible)

- Non-governmental organisation (NGO)
- Trade union
- Employers' organisation
- Social and professional organisation
- Faith-based, religious, philosophical or non-confessional organisation
- University or other qualified experts of European/international body/organisation
- Other: _____

38d. What is your organisation mainly engaged in (a minimum of one and a maximum of four selections are possible):

- Advocacy
- Campaigns
- Education and awareness raising
- Legal cases (litigation) on behalf of plaintiffs/strategic litigation
- Representation of victims, victim support, counselling (legal, psycho-social)
- Gender equality or women's empowerment
- Research, data collection
- Service provision: social integration/social services/health projects/refugee support
- Targeted work with the media
- Finance-related activities, including grants – "core funding" of your organisation's infrastructure
- Other, please specify: _____

38e. Please select the main theme(s)/field(s) your organisation is operating in (a minimum of one and a maximum of five selections are possible):

- Access to justice, including victims of crime
- Age discrimination/youth
- Age discrimination/older people
- Disability
- Legal advice/litigation with respect to discrimination
- Economic and social rights

- Education
- Gender
- Health
- Information society, privacy, data protection
- Judicial and police cooperation
- LGBTI
- Immigration, asylum and return, integration
- Poverty eradication
- Racism, xenophobia and related intolerance
- Religion/freedom of religion
- Rights of the child
- Roma integration
- Sexual and reproductive rights
- Women
- General human/fundamental rights
- Other, please specify: _____

38f. How many paid employees does your organisation have?

- 0
- 1-5
- 6-15
- 16-50
- 51-100
- 101-500
- More than 500
- Don't know

38g. How many volunteers work with your organisation?

- 0
- 1-5
- 6-15
- 16-50

- 51-100
- 101-500
- More than 500
- Don’t know

Further information:

For more on the GDPR and on data protection, see:

- *Handbook on European data protection law – 2018 edition (2018),* http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law
- *Fundamental Rights Report 2018,* https://fra.europa.eu/en/publication/2018/fundamental-rights-report-2018

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel: +43 158030-0 – Fax: +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Publications Office of the European Union

Print: ISBN 978-92-9474-539-2, doi:10.2811/135632
PDF: ISBN 978-92-9474-540-8, doi:10.2811/538633

TK-04-19-192-EN-C (print); TK-04-19-192-EN-N (PDF)