FREEDOMS

Access to data protection remedies in EU Member States

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

This report addresses matters related to the protection of personal data (Article 8) and the right to an effective remedy (Article 47) falling under Titles II 'Freedoms' and VI 'Justice' of the Charter of Fundamental Rights of the European Union.

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Photo (cover & inside) : SXC

More information on the European Union is available on the Internet (http://europa.eu).

FRA – European Union Agency for Fundamental Rights
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel.: +43 158030-0 – Fax: +43 158030-699
Email: info@fra.europa.eu – fra.europa.eu

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2013

ISBN 978-92-9239-460-8
doi: 10.2811/69883

Printed in Italy

PRINTED ON PROCESS CHLORINE-FREE RECYCLED PAPER (PCF)

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Access to data protection remedies in EU Member States

Foreword

To uphold fundamental rights, individuals must have access to remedies that are both effective in law and in practice. This European Union Agency for Fundamental Rights (FRA) report presents the findings of a sociolegal research project on the main challenges and barriers that individuals encounter when seeking remedy after a data protection violation. It supplements FRA's previous research on the role of national data protection authorities (DPAs) in the fundamental rights landscape as well as FRA's Opinion on the proposed EU data protection reform package.

To understand how data protection violations are remedied in practice, FRA interviewed key players involved in the remedial process: victims of the data protection violations, representatives of the DPAs, non-governmental organisations (NGOs) and legal professionals.

This FRA report identifies factors hampering the effectiveness of existing remedy mechanisms. It highlights a persistent lack of knowledge about the protection of personal data. Individuals therefore do not understand what constitutes a data protection violation. When they are informed, they address their complaint to national DPAs, which are key players in the fundamental rights landscape in the European Union. These, however, often suffer from a lack of adequate resources and powers. FRA findings also show that judges and lawyers are not aware of data protection rules. Too few are specialised in this area of law, rendering judicial enforcement of this fundamental right difficult. In the absence of specialised NGOs, the burden falls on DPAs to effectively guarantee data protection.

In offering suggestions for the EU and its Member States on how to strengthen the role of DPAs and legal professionals, as well as civil society organisations, this report contributes to making justice in the area of data protection more accessible across the EU. It comes as timely advice given the ongoing reform of the data protection rules in Europe and it will hopefully contribute to this important reform process.

Morten Kjaerum
Director

Acronyms

CCTV	Closed-circuit television
DPA	Data protection authority or independent supervisory authority
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EU	European Union
GIODO	Inspector General for the Protection of Personal Data (Poland)
NFP	National focal point
NGO	Non-governmental organisation
PHSO	Parliamentary and Health Service Ombudsman

Contents

Executive summary

Introduction

This FRA report encompasses legal and social fieldwork research on European Union (EU) Member States' remedies in the area of data protection. By offering an EU-wide legal comparative analysis of data protection remedies, it gives an insight into the availability of remedies in each EU Member State. It also shows the challenges people encounter when seeking remedies following a data protection violation in a selected number of Member States.

This research aims to provide evidence on the use and application of data protection remedies in the EU Member States studied; to identify the main challenges faced by different actors; and to identify possible improvement in access to data protection remedies.

Policy context

The report focuses on two fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union: the right to the protection of personal data (Article 8) and the right to an effective remedy before a tribunal (Article 47). These two fundamental rights should be analysed together because the right to an effective remedy cannot be dissociated from the need to effectively enforce all fundamental rights, including the protection of personal data.

A number of remedy mechanisms are available to victims of data protection violations. The spectrum ranges from assistance from various non-judicial bodies and national data protection authorities (DPAs) to the courts, including administrative as well as civil and criminal proceedings.

FRA's research focuses on DPAs and the judiciary. It touches on the role of other non-judicial bodies such as national ombudsmen or other administrative authorities that can promote data protection rights and provide remedies for violations. However, the number of non-judicial bodies reported to be operating in the area of data protection is small and many non-judicial bodies have only limited powers to offer remedies.

In addition to the Charter of Fundamental Rights of the European Union guaranteeing the right to an effective remedy and the right to the protection of personal data, the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is the keystone of EU legislation guaranteeing the right to personal data protection in EU Member States. It requires each Member State to set up an independent supervisory authority and provide for the right of every person to a judicial remedy for any violation of the rights guaranteed by the national law applicable to the processing in question. The directive also requires Member States to provide for a remedy against decisions by a supervisory authority which give rise to complaints. Thereby, it acts as a tool to provide access to justice for this area of law. The Data Protection Directive allows Member States to implement these requirements into their own data protection systems. This results in a variety of possible outcomes depending on the Member State in which remedy is sought.

The European Commission has proposed a comprehensive data protection reform package, bearing in mind the need for more effective enforcement of the fundamental right to personal data protection. This report does not assess that reform, but its findings provide evidence to inform and contribute to the reform.

Key findings

The legal analysis found that DPAs across EU Member States can issue orders to rectify violations and impose sanctions ranging from warnings and fines to the revocation of licences. Sanctions that DPAs are empowered to impose differ between Member States. In most of them, judicial authorities can award damages for violations, although guidelines on award amounts vary. FRA data shows that in almost all Member States criminal sanctions can be imposed, in the form of a fine or imprisonment. The duration of a sentence and the amount of a fine also vary across Member States.

Most data protection violations in the 16 EU Member States were thought to arise from internet-based activities, direct marketing and video surveillance with closed-circuit television (CCTV) cameras. Institutions responsible include governmental bodies, law enforcement agencies and financial and health institutions. The complainants and non-complainants interviewed defined the damage from data protection violations as psychological and social. They described emotional distress, offence, insecurity or damage to reputation as well as impact on their relations with other people. Fieldwork participants also reported financial damages but less frequently.

Most complaints were lodged with the national DPAs and very few went through judicial procedures. Most individuals will not pursue cases before a court because of the lengthy, time-consuming and complicated procedures and costs involved. This view is widely shared by judges and practising lawyers. Reasons why people more often lodge complaints with national DPAs include the following factors: DPAs do not necessitate high costs; their complaint procedure is shorter and less complex; and the procedure does not demand legal representation.

Financial compensation was not a motivating factor to seek redress for the fieldwork participants. Instead, most complainants and non-complainants say they sought redress to ensure that similar data protection violations do not recur.

Most interviewees worry about the lack of legal assistance available. Judges and lawyers interviewed noted that there are too few data protection professionals; they also recommended training and more specialisation in data protection law. This lack of data protection experts was also a problem in looking for and trying to access interviewees during the fieldwork. People also raised concerns over the lack of financial and human resources available to DPAs and intermediary organisations specialised in the area of data protection. Many individuals reported difficulty in obtaining information about procedures and insufficient knowledge of remedies. Most interviewees who had suffered a data protection violation said they lacked information; only a minority, defined as 'well-informed', said they had information thanks to their professional background (mainly legal) or previous experience.

The general public needs to know more about data protection violations, existing remedies and support, as FRA findings show. There is also a need to ensure that professionals dealing with data protection issues are aware of developments in the field and legislation. Fieldwork also indicates that DPAs and intermediaries lack adequate resources.

Methodology

Based on FRA legal research analysing laws and rules of procedure in each of the 28 EU Member States, this report provides a comparative analysis of the national legal frameworks in the area of data protection remedies. The social fieldwork is based on qualitative research in the following 16 EU Member States: Austria, Bulgaria, the Czech Republic, Finland, France, Germany, Greece, Hungary, Italy, Latvia, the Netherlands, Poland, Portugal, Romania, Spain and the United Kingdom.

Over 700 individuals from six target groups were interviewed or took part in the focus groups. These six target groups were complainants; non-complainants such as alleged victims of data protection violation who decided against seeking a remedy; judges; staff of DPAs; intermediaries, including staff members of civil society organisations; and practising lawyers.

The report presents an overview of the legal framework and the procedures in place. An assessment of the implementation of the data protection remedies as perceived by the main actors is made by looking at a number of related issues, namely fieldwork findings assessing the accessibility and availability of support structures. These structures help affected individuals to access procedures for remedies (both judicial and alternative) in the field of data protection. The report also presents how interviewees perceived costs, deadlines to be observed and the burden of proof. In addition, it seeks to identify barriers met in using and applying the remedies in the field of data protection, including the perspectives of individual complainants and other relevant actors. It also seeks to identify areas for improvement in accessing data protection remedies.

Opinions

This report identifies potential for concrete improvement in a number of areas. The EU institutions, EU Member States and mechanisms involved in implementing data protection remedies could all take action to improve the present situation. The European Union Agency for Fundamental Rights (FRA) has formulated the following opinions based on the findings in this report and previous research as ways forward to improve the availability and quality of remedies available to victims of data protection violations in the EU.

Strengthening the role of data protection authorities

Data protection authorities (DPAs), the main actors protecting data protection rights, play a crucial role in processing the overwhelming majority of data protection complaints. Further action is needed to ensure that access to DPAs is effective in practice.

The independence of DPAs must be strengthened through a reform of EU legislation. They should have enhanced powers and competences, supported by adequate financial and human resources, including diverse and qualified professionals, such as trained information technology specialists and qualified lawyers.

The European Parliament and the Council of the European Union are proposing regulation to protect individuals with regard to the processing of personal data and the free movement of such data. This General Data Protection Regulation seeks to further harmonise data protection legislation, and to further strengthen the ability of DPAs to remedy violations.

Data protection strengthening could include safeguards for effective enforcement of their decisions and reasonable length of procedures (see also, in the specific context of non-discrimination, the 2012 FRA report on *Access to justice in cases of discrimination in the EU: steps to further equality*). This would enable DPAs to remain the preferred point of access for remedying data protection violations, while streamlining the existing remedy avenues and decreasing overall costs, delays and formalities (see the 2012 *FRA Opinion on the proposed data protection reform package*).

To strengthen their authority and credibility, DPAs should play an important role in the enforcement of the data protection system, by having the power to either issue sanctions, including fines, or procedures that can lead to sanctions (see also the 2010 FRA report on *Data protection in the European Union: the role of national data protection authorities*).

This opinion is in line with the findings in the context of other non-judicial bodies, such as equality bodies, as highlighted in the 2013 FRA Opinion on the EU equality directives (p. 3):

"The degree to which complaints procedures fulfil their role of repairing damage done and acting as a deterrent for perpetrators depends on whether dispute settlement bodies are able to issue effective, proportionate and dissuasive sanctions" and *"allowing civil society organisations, including equality bodies, to bring claims to court or conduct investigations [...] could help facilitate enforcement."*

Data protection authorities are encouraged to be more transparent, as well as to communicate effectively with the general public, providing necessary information and easing access to remedies in practice. In addition, as highlighted by the 2010 FRA report on the role of national data protection authorities in the EU, DPAs "should promote closer cooperation and synergy with other guardians of fundamental rights [...] in the emerging fundamental architecture of the EU" (p. 8). Such steps would improve the image of DPAs, their perceived effectiveness and independence and the trust of the general public.

Enhancing the role of lawyers and judges

Legal professionals rarely deal with data protection cases, so they are not aware of the applicable legal procedures and safeguards. There is a lack of judges specialised in this area.

The EU could financially support training activities for lawyers and judges on data protection legislation and its implementation at Member State level. EU Member States should seek to strengthen the professional competence of judges and lawyers in the area of data protection, providing training programmes and placing added emphasis on data protection issues in the legal curriculum. This would increase the availability of sufficiently qualified legal representation.

Strengthening professional competence would also help reduce the length of proceedings. The gap in such competence is one of the barriers to seeking redress before courts, as confirmed by the 2011 FRA report on *Access to justice in Europe: an overview of challenges and opportunities*, and by the findings of this fieldwork.

Strengthening the role of civil society organisations

The report highlights the importance of intermediary organisations as a source of information, advice, legal assistance and representation. However, only a very limited number of civil society organisations are able to offer comprehensive services for victims of data protection violations. The EU and its Member States should increase funding for civil society organisations and independent bodies in a position to assist such victims seeking redress.

Victims are often reluctant to bring claims. Allowing civil society organisations to bring claims to court or conduct investigations could constitute an important step to help enforcement. As already emphasised in other FRA reports and opinions, and confirmed by the findings of this report, strict rules relating to legal standing prevent civil society organisations from taking a more direct role in litigation in cases of fundamental rights violations (see the 2011 FRA report *Access to justice in Europe: an overview of challenges and opportunities* and the 2012 FRA report *Access to justice in cases of discrimination in the EU: steps to further equality)*.

The 2012 FRA Opinion on the proposed data protection reform package in particular says that the EU should consider further relaxing legal standing rules to enable organisations acting in the public interest to lodge a data protection complaint in cases where victims are unlikely to bring actions against a data controller, given the costs, stigma and other burdens they could be exposed to. As underlined in FRA reports on access to justice, this would also ensure that cases of strategic importance are processed, thus enhancing the culture of compliance with data protection legislation. Such broadening of the legal standing rules should be accompanied by additional safeguards preserving the right balance between the effective access to remedies and abusive litigation. The Commission has proposed a form of representative collective redress in the General Data Protection Regulation.

Reducing costs and easing the burden of proof

Victims of data protection violations are dissuaded from pursuing cases for several reasons, including costs and difficulties associated with proving data protection violations.

EU Member States should consider promoting support through legal advice centres or pro bono work. These support mechanisms should be complementary to, and not a substitute for, an adequately resourced legal aid system.

Rules on the burden of proof should be streamlined, especially in cases concerning internet-based activities.

Raising awareness

Victims lack awareness of data protection violations and of available remedies. These findings of the FRA fieldwork confirm existing FRA research conclusions.

As recognised by the 2010 FRA report on *Data protection in the European Union*, awareness-raising on data protection legislation is an important task for relevant institutions, such as national DPAs. A similar lack of awareness was highlighted in the 2012 FRA report on *Access to justice in cases of discrimination* and the 2013 FRA Opinion on the EU equality directives, in relation to EU non-discrimination legislation. From the general public to judges, awareness-raising measures are needed. Knowledge about support organisations that complainants can turn to when lodging data protection complaints needs to be significantly increased throughout the EU.

The EU could promote and possibly financially support awareness-raising campaigns at EU Member State level. To raise national practitioners' awareness of the data protection rules, the FRA, together with the Council of Europe and the European Court of Human Rights, prepared a Handbook on European data protection law.

EU Member States could consider taking the necessary steps to increase the public's awareness of the existence and functioning of available complaint mechanisms, particularly DPAs. In addition, DPAs should pay particular attention to cultivating their public profile as independent guardians of the fundamental right to data protection, and should enhance their awareness-raising activities on data protection.

Introduction

Background

This report gives the results of legal and social fieldwork research on EU Member States' remedies in the area of data protection. It has two main aims. The first is to provide insight into the use and application of data protection remedies, and the obstacles faced by people whose data protection has been violated, and those who provide representation and support, in their attempts to gain or to implement the available remedies. The second is to explore what incentives exist to encourage potential complainants to try to access the remedies, and to identify ways forward.

This report provides an EU-wide comparative analysis of the remedies. This is intended to ensure individuals' rights in the area of data protection. It focuses on the juncture of two fundamental rights enshrined within the Charter of Fundamental Rights of the European Union (the Charter): the right to an effective remedy (Article 47 of the Charter) and the right to the protection of personal data (Article 8 of the Charter). The right to an effective remedy cannot be separated from the effective enforcement and implementation of all other fundamental rights, including data protection. Given this, it is important to look at both fundamental rights together.

There are a number of mechanisms available to victims of data protection violations. In addition to seeking remedy before the courts – in terms of administrative as well as civil and criminal proceedings – national DPAs and non-judicial bodies offer a further step.

The Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)[1] guarantees the availability of data protection remedies in the EU Member States by requiring each Member State to set up one or more independent supervisory authorities. It also establishes the right of every person to a judicial remedy against decisions by a supervisory authority which give rise to complaints.

The findings of a 2011 Eurobarometer survey highlight that Europeans are concerned about data protection issues. They are, however, uninformed about the availability of remedies in case of data protection violations, despite EU legislation enshrining the right to redress for data protection violations, and seeking to ensure appropriate mechanisms to provide for it. According to the 2011 Eurobarometer survey on *Attitudes on data protection and electronic identity in the European Union*,[2] most of the Europeans (74 %) surveyed saw disclosing personal information as an increasing part of modern life. In addition, 70 % expressed concern that their personal data held by companies may be used for a purpose other than that for which it was collected. Only 33 % are aware of the DPA's existence. This FRA report confirms those findings.

Bearing in mind the need for more effective enforcement of the fundamental right to personal data protection, the European Commission has proposed a data protection reform package. It consists of a proposal for a General Data Protection Regulation[3] replacing the Data Protection Directive and a proposal for a General Data Protection Directive[4] replacing the Council of the EU's Data Protection Framework Decision.[5] This report does not assess the reform but FRA findings are supporting the efforts of the EU legislature to secure an effective data protection framework in the EU.

FRA work on data protection

Previous FRA work has focused on related data protection issues, including the FRA Symposium of 2010 on strengthening the fundamental rights architecture in

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281 (*Data Protection Directive*).

2 The 2011 Special Eurobarometer survey was conducted in the 27 EU Member States between the end of November and mid-December 2010. A total of 26,574 Europeans aged 15 and over were interviewed. All interviews were conducted face to face in people's homes and in the appropriate national languages, see European Commission (2011).

3 European Commission (2012a), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

4 European Commission (2012), *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, COM(2012) 10 final, Brussels, 25 January 2012.

5 Council of the European Union (2008), Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L 350.

the EU, addressing the role of data protection authorities[6] and the FRA Symposium of 2012 on data protection.[7] In addition, a number of FRA reports are especially relevant. These include the 2010 FRA report on data protection in the European Union,[8] the 2012 *FRA Opinion on the proposed data protection reform package*[9] and the FRA report on the independence and staffing of DPAs.[10]

Furthermore, the 2011 FRA report on *Access to justice in Europe: an overview of challenges and opportunities*[11] and the 2012 FRA report on *Access to justice in cases of discrimination in the EU*[12] deal specifically with access to justice in the EU Member States in general as well as in cases of non-discrimination. The findings of these studies led to a number of opinions that are applicable to the current issue of access to remedies in the area of data protection, as confirmed by the findings of this research. With regard to the structures and procedures of remedy mechanisms, the reports on access to justice called on the EU to ensure that equality bodies and other institutions with an equality remit are sufficiently independent and well resourced. They also called for non- and quasi-judicial bodies to be given additional powers to deal with violations, in particular the ability to issue sufficiently substantive sanctions. This was also reiterated in the 2013 FRA Opinion on the EU equality directives.[13] With regard to the support available for complainants, the reports called for an improvement in the availability of legal advice and expertise, as well as raising awareness of discrimination-related issues and the remedies available in case of discriminatory acts. With regard to proceedings, the reports called for, among other things, a shortening of the length of cases. They offered the opinion that more should be done to permit complaints by multiple complainants, as well as to ensure that civil society organisations can bring claims on behalf of victims of discriminatory acts. These opinions were formulated in the area of access to justice regarding discrimination, but can also be applied to data protection, as the fieldwork data show.

The legal research, i.e. the comparative analysis across the EU28, assesses the current legal framework in place and the extent to which access to an effective remedy already exists. It is conducted by analysing laws and rules of procedure in each of the 28 EU Member States.

6 See FRA (2010).
7 FRA (2012a), *European Union data protection reform: new fundamental rights guarantees,* FRA Symposium Report, 10 May 2012.
8 FRA (2010).
9 FRA (2012b).
10 FRA (2014 forthcoming).
11 FRA (2011a).
12 FRA (2012c).
13 FRA (2013).

The evidence collected through the social fieldwork is analysed in the light of the existing legal instruments in place at international, European and national levels to give redress in the area of data protection.

The report also profited from the input from the Article 29 Working Party as well as the Commission which were consulted in the course of the research.

The social research

The methodology applied to the social research does not aim to provide data on the overall prevalence of data protection violations and their outcomes. Instead, the data collected provide a better insight and deeper understanding of the experiences and needs of the individuals who have suffered data protection violations. It also provides an assessment of the procedures available and different elements of the remedies from the perspective of different actors involved, such as lawyers, judges and representatives of DPAs or other organisations providing support for the subjects of violations.

Although this report provides a comparative analysis of the national legal frameworks in the area of data protection remedies across the 28 EU Member States, the social fieldwork is based on qualitative research in 16 Member States: Austria, Bulgaria, the Czech Republic, Finland, France, Germany, Greece, Hungary, Italy, Latvia, the Netherlands, Poland, Portugal, Romania, Spain and the United Kingdom. These 16 Member States were selected to ensure a geographical spread, taking into account budget limitations at the time of the research.

FRA's multidisciplinary research network, FRANET, composed of national focal points (NFPs) in each EU Member State, carried out the fieldwork. National reports presented the data collected, and the comparative report was compiled on the basis of the national ones.

The fieldwork, carried out from April to September 2012, studied over 700 individuals from the six target groups. The data were collected through semi-structured interviews and focus group discussions with the representatives of major actors in the field. In each EU Member State covered by the fieldwork, there were semi-structured interviews with the representatives of the following target groups:

- individuals who have experienced data protection remedies, i.e. those who have initiated a legal process (henceforth referred to as 'complainants') and individuals who intended to seek a remedy for a perceived data protection violation but decided not to pursue a legal process (henceforth referred as 'non-complainants') (in total, 351 interviews);

- judges (or prosecutors) directly tasked with adjudicating in the context of redress mechanisms in the field of data protection at various relevant courts (civil, administrative, criminal, etc.) (84 interviews).

Focus group discussions were held with representatives of the national DPAs, practising lawyers and intermediaries. Intermediaries included individuals working at support organisations for the individuals subjected to the data protection violations, including relevant consumer protection groups, employee organisations, trade unions, complaints organisations or other non-governmental or civil society organisations, and other professionals involved in advising and supporting complainants.[14] When lawyers represented intermediary organisations, their opinions and perceptions were analysed as those of intermediaries and not lawyers as a separate target group. In all the countries researched, three focus group discussions were organised and all the participants in these groups were required to be advising or directly dealing with subjects of data protection violations who seek redress.

The choice of data collection method was based on the research subject, the topic's sensitivity and the accessibility of the target group. For example, individual interviews were carried out with complainants and non-complainants because their personal experiences were discussed and shared. The judges were interviewed individually because they were hard to reach in terms of time, location and the small number of professionals available. Other professionals targeted were invited to the focus group discussions, which were more effective and reasonable ways to collect data. The semi-structured interviews and focus group discussions were designed to obtain detailed accounts of the following issues:

- perceptions of effectiveness of the data protection remedies;
- difficulties faced in accessing redress mechanisms, including costs, legal aid, deadlines to be observed, burden of proof, etc.;
- assessment of the quality of the procedures regarding the data protection remedies;
- assessment of the possibilities offered by the data protection remedies;
- perceptions of the intermediaries and representatives of data protection authorities concerning the process, application and use of the remedies;
- identification of areas for possible improvements for the remedies available.

Interview and discussion guidelines followed a similar structure in order to capture the opinions of different actors involved in redress about the same issues, with some adjustments in relation to their specific experiences.

Interviews lasted on average about one hour. Most interviews were conducted face to face, with a few interviews undertaken by telephone to suit the needs of the interviewee and the researcher (most of these were with judges who worked in different geographical locations). In one instance, an interview was conducted by email.

Detailed information about the interviewees and issues faced accessing the interviewees is provided in the annex.

Peer review of methodology and facts was an integral part of this research project. During the project methodology development, two stakeholder meetings took place. The stakeholder meeting held in February 2011 brought together key experts from the EU level (European Commission, European Data Protection Supervisor, Council of Europe), national government agencies, DPAs, NGOs and universities. Stakeholders at the meeting for the EU Member States, held in February 2012, gave advice and commented upon the research design, and contributed contact details for interviewees through the national DPAs and other bodies in each country. Representatives of the national DPAs and NGOs peer-reviewed this report.

Presentation of the findings

The report provides an overview of standards on effective data protection remedies across the EU Member States (Chapter 1). It then focuses on data protection remedies available at national level in the 28 Member States (Chapter 2) before examining the experiences and views of the different actors in the field of data protection (Chapters 3 and 4).

14 In cases where it was difficult to ensure a reasonable number of participants (because of geographical distances, timing, too few organisations or professionals available and other reasons), focus group discussions were replaced by group interviews or an equivalent number of one-to-one interviews.

An assessment of the use and application of the data protection remedies considers structural, procedural and support aspects. For example, the structural aspects deal with the complaint mechanisms and legislation, and the related research findings are presented in Chapter 1. The procedural aspects cover remedies' effectiveness and timely resolution. These aspects are dealt with by assessing the remedies' availability and accessibility, length of proceedings and costs involved. The support elements include awareness of rights, legal aid available and information available.

If relevant and if the information is available, the report presents opinions of different target groups interviewed. The report focuses on comparative findings. The EU countries listed (either in the text or in brackets) serve as examples rather than an exhaustive list of countries where certain findings were observed. Examples of practices or standards followed, which were collected during the fieldwork, appear interspersed throughout the text of the report. The report also uses quotes from some of the interviews. At the end of each section of Chapters 2, 3 and 4, the key findings are presented.

1

Effective remedy: the standards

1.1. The right to an effective remedy

This report focuses on the juncture of two fundamental rights: the right to an effective remedy and the right to the protection of personal data. It is important to look at these two fundamental rights together because the right to an effective remedy, which represents one of the core elements of the access to justice,[15] cannot be left out when analysing the need for the effective enforcement and implementation of all other fundamental rights, including data protection. A number of mechanisms exist for those seeking remedy for a violation of their data protection rights, namely DPAs, the judiciary – through civil, administrative and criminal proceedings – and other intermediary organisations.[16] Each of them has varying powers to offer an effective remedy. Both the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[17] (Convention 108), together with its Additional Protocol on supervisory authorities and transborder data flows (181),[18] and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)[19] have shaped the legal frameworks in place across the EU Member States.

This section offers a comparative analysis across the EU28, assessing the current legal framework in place and the extent to which access to an effective remedy already exists.

The right to an effective remedy is the main procedural guarantee touched on by this report[20] and is enshrined within both the Charter of Fundamental Rights of the European Union (EU Charter) and the European Convention on Human Rights (ECHR). Article 47(1) of the EU Charter sets out that:

"Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article."

The Presidium of the Convention, which drafted the EU Charter,[21] provided the following guidance on the interpretation of Article 47(1) of the Charter, basing it on Article 13 of the ECHR, which reads:

"Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

The European Court of Human Rights (ECtHR) explained the object of Article 13 of the ECHR in the following terms:

15 FRA (2011a).

16 See Chapter 5 'Equality and non-discrimination' in FRA's Annual report (2011b), pp. 15–16, and also Chapter 5 'The data subject's rights and their enforcement' in FRA's and Council of Europe's *Handbook on European data protection law* (2014).

17 CoE (1981).

18 CoE (2001).

19 See OJ 1995 L 281, p. 31.

20 FRA (2011b).

21 Explanations relating to the Charter of Fundamental Rights, OJ 2007 C 303, p. 17, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF.

"The object of Article 13, as emerges from the travaux préparatoires, is to provide a means whereby individuals can obtain relief at national level for violations of their Convention rights before having to set in motion the international machinery of complaint before the Court."[22]

Indeed the Court has further reiterated that "Article 13 of the Convention guarantees the availability at the national level of a remedy to enforce the substance of the Convention rights and freedoms in whatever form they might happen to be secured in the domestic legal order." [23] Closely related to the right to an effective remedy is the right to a "fair and public hearing within a reasonable time by an independent and impartial tribunal established by law", as guaranteed by Article 6 of the ECHR.[24]

Traditionally, before Article 47 of the Charter became legally binding, the Court of Justice of the European Union used the constitutional traditions common to the EU Member States, as well as Articles 6 and 13 of the ECHR above, as a basis for the right to obtain an effective remedy before a competent court.[25] Within the EU legal order, the right to effective legal protection equally covers access to the EU courts as well as access to national courts and tribunals for the enforcement of rights derived from EU law.

A broad interpretative reading of Article 47(1) of the EU Charter and Article 13 of the ECHR indicates that other forms of remedial mechanisms apart from judicial remedies may also be available and considered effective.[26] In making reference to securing a remedy for violations "in whatever form", the ECtHR indicates a willingness to interpret the right to an effective remedy broadly, incorporating not only judicial remedy mechanisms, but also other remedial mechanisms. Article 47(1) of the EU Charter and Article 13 of the ECHR do not limit the provisions to judicial remedy; instead, they prefer to secure a remedy before a tribunal and a national authority respectively.

22 ECtHR, *Kudla v. Poland*, No. 30210/96, 26 October 2000.

23 ECtHR, *Lyanova and Aliyeva v. Russia*, Nos. 12713/02 and 28440/03, 2 October 2008, para. 134.

24 ECtHR, *Kudla v. Poland*, No. 30210/96, 26 October 2000, paras. 146–156; ECtHR, *I. v. Finland*, No. 20511/03, 3 April 2007.

25 CJEU, Joined Cases C-402/05 P and C-415/05 P, *Kadiand Al Barakaat International Foundation v. Council and Commission*, 3 September 2008, para. 335.

26 One of the stipulations that the relevant case law includes in this respect is the independence and impartiality of the body in question (see ECtHR, *Klass and Others v. Germany*, Series A No. 28, 6 September 1978, para. 67). See, for general principles of tribunals' independence, ECtHR, *Kleyn and Others v. Netherlands*, Nos. 39343/98, 39651/98, 43147/98 and 46664/99, 6 May 2003, para. 190. See also CJEU, C-506/04, *Graham Wilson v. Ordre des avocats du barreau de Luxembourg*, 19 September 2006, paras. 47–53 ; CJEU C-196/09, *Paul Miles and Others v. Écoles européenne*, 14 June 2011, para. 37.

For the purposes of this report, the right to an effective remedy as set out in the EU Charter and ECHR incorporates access not only to judicial remedies, but also, in the area of data protection, to those operated by DPAs or by other non-judicial authorities. The EU Charter, as well as Convention 108 and its Additional Protocol, requires the establishment of DPAs to monitor the correct application of data protection legislation. The ECtHR recognised in the *Leander v. Sweden* case that "the 'national authority' referred to in Article 13 need not be a judicial authority in the strict sense."[27] As previously noted, Article 13 guarantees the availability of a remedy at national level in whatever form the domestic legal order may provide for. Thus, its effect is to require the provision of a domestic remedy allowing the "competent national authority" both to deal with the substance of the relevant Convention complaint and to grant appropriate relief.[28] Thus, DPAs – as well as intermediary organisations such as ombudsperson institutions or other non-judicial bodies – are considered national authorities. Where secret surveillance is concerned, objective supervisory machinery may be sufficient as long as the measures remain secret.[29] However, the remedy must be "effective" in practice as well as in law. Thus, the powers and procedural guarantees an authority possesses are relevant in determining whether or not the remedy before it is effective.

This broad interpretation was recently confirmed in a proposed Agreement between the European Union and the Russian Federation on drug precursors.[30] According to the proposal, a redress mechanism for data protection violations shall be in place so that each EU Member State ensures that a data subject who considers that they have been a victim of a data protection violation "shall have the right to an effective administrative remedy before a competent authority and a judicial remedy before an independent and impartial tribunal". The proposal further provides that:

"Any such infringements or violation shall be subject to appropriate, proportionate and effective sanctions including compensation for damages suffered as a result of an infringement of data protection rules. Where data protection provisions are found to have been violated sanctions including compensation are to be imposed in accordance with applicable domestic rules."

Different judicial and non-judicial paths offer different forms of remedies and, in addition to financial

27 ECtHR, *Leander v. Sweden*, Series A No. 116, 26 March 1987.

28 See ECtHR, *Peck v. the United Kingdom*, No. 44647/98, 28 January 2003, para. 99, and ECtHR, *Kennedy v. the United Kingdom*, No. 26839/05, 18 May 2010, para. 196.

29 ECtHR, *Rotaru v. Romania*, No. 28341/95, 4 May 2000, para. 69.

30 European Commission (2013a), Annex II – Data protection definitions and principles, p. 15.

compensation, these can include orders to annul decisions taken by other authorities, rectify violations, implement specific security measures, rectify or erase information or impose fines or indeed criminal sanctions (see further Chapter 2).

1.2. A fundamental right to personal data protection

Article 8 of the Charter establishes data protection as a fundamental right distinct from the right to private life under Article 7 of the Charter.[31] According to Article 8 of the Charter:

"Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

As set out in the explanations relating to the Charter,[32] Article 8 of the Charter is based on Article 286 of the Treaty establishing the European Community (replaced by Article 16 of the Treaty on the Functioning of the European Union) and the Data Protection Directive, as well as on Article 8 of the ECHR and on Convention 108.

The Data Protection Directive has been an important secondary instrument of the European Union to guarantee data protection in the EU Member States, and a tool to provide access to justice for this area of law. The purpose of the directive is both to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States.[33]

The directive contains important provisions on remedy mechanisms in the area of data protection and establishes minimum standards which need to be met by all EU Member States. It states that Member States shall adopt suitable measures to ensure the full implementation of the directive and shall, in particular, lay down the sanctions to be imposed in case of infringement of the directive. This encompasses all kinds of sanctions, including possible criminal sanctions.

The provision of remedy mechanisms is guaranteed by Article 22 of the directive, which establishes that EU Member States shall, without prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, provide for the right of every person to a judicial remedy for any violation of the rights guaranteed him by the national law applicable to the processing in question.

With regard to the sanctions available in such proceedings, Article 23 of the directive states that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted implementing the directive is entitled to receive compensation for the damage suffered. Any damage which a person may suffer as a result of unlawful processing should be compensated for by the controller or processor. However, the controller or processor may be exempted from liability if they prove that they are not responsible for the damage, in particular where they establish fault on the part of the data subject or in case of force majeure. The concept of damage is to be broadly interpreted, in the light of the case law of the Court of Justice of the European Union, as meaning both material and immaterial damage.

Article 24 of the directive states that EU Member States shall adopt suitable measures to ensure the full implementation of the directive and shall, in particular, lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to the directive. The directive does not detail the categories of sanctions or whether and, if so, what sanctions could be imposed by DPAs or by other authorities or by the courts.

Further powers are granted specifically to the independent[34] DPAs in each EU Member State, with Article 28 stating that DPAs shall be endowed with:

- investigative powers;
- effective powers of intervention, such as powers to order the blocking, erasure or destruction of data, to impose a temporary or permanent ban on processing, to warn or to admonish;
- the power to engage in legal proceedings or to bring violations of the directive to the attention of the judicial authorities.

The directive spells out that each supervisory authority shall hear claims also when lodged by an association representing the individual, but it does not provide the

31 See FRA and Council of Europe (2014).

32 Explanations relating to the Charter of Fundamental Rights, OJ 2007 C 303, p. 17.

33 See Chapter 1 'Context and background of European data protection law' in FRA and Council of Europe (2014).

34 For the requirement of "complete independence", see CJEU, C-518/07, *European Commission v. Germany*, judgment of 9 March 2010.

possibility for associations to represent data subjects in court cases.

The directive confirms that DPAs have a fundamental role to play in providing remedy for data protection violations. Although the directive grants the DPA powers to order actions aimed at remedying violations, the 2012 Evaluation of the implementation of the Data protection Directive[35] notes that, in several EU Member States, DPAs are not endowed with the full range of powers to conduct investigations, intervene in data-processing operations and engage in legal proceedings. The evaluation carried out by the Commission points out that the divergent powers held and approaches to enforcement taken by the individual DPAs causes not only problems for the data subjects, who do not enjoy the same level of enforcement in each Member State, but also uncertainties for controllers, particularly when operating in several Member States.

Mindful of the need for a more comprehensive and coherent policy on the fundamental right to personal data protection, on 25 January 2012 the European Commission put forward the Data Protection Reform package with two specific proposals: a draft regulation setting out a general EU framework for data protection (hereafter draft Regulation);[36] and a draft directive on protecting personal data processed for the purpose of prevention, detection, investigation or prosecution of criminal offences and related judicial activities (hereafter draft directive).[37] In the Explanatory Memorandum of the proposed regulation,[38] the European Commission asserted that, although the current framework remains sound as far as its objectives and principles are concerned, it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated particularly with online activity. The proposed regulation seeks to build a stronger and more coherent data protection framework in the EU. Adopting changes in the form of a regulation would ensure further harmonisation of data protection law across the EU Member States and provide coherence on data protection issues within the EU.

In seeking to ensure further harmonisation and a stronger data protection framework, the draft regulation builds on the provisions of Article 28 of the Data Protection Directive, enshrining through Article 53 of the draft regulation the powers of the DPAs, including the ability to warn or admonish; to order the rectification, erasure or destruction of data; to impose a temporary or definitive ban on processing; to suspend data flows to a recipient in a third country or to an international organisation; and to issue opinions on any issue related to the protection of personal data.

Article 79 of the draft regulation contains a new harmonised obligation for EU Member States to empower DPAs to impose administrative fines. These fines can be up to €1 million, or up to 2 % of the annual worldwide turnover for enterprises.

The proposed regulation adresses various administrative and judicial remedies, including compensation, interim measures, penalties, administrative sanctions and criminal sanctions. If adopted, these new provisions would significantly increase the abilities of the DPAs to impose sanctions on controllers or processors for data protection violations under EU law.

The extent to which the sanctions provided for in the proposed regulation are already available in EU Member States is addressed below. As the following chapter indicates, since the provisions of the Data Protection Directive concerning remedies, sanctions and liability only set the objective criteria to be followed, a number of differences exist between the national laws on data protection.

35 European Commission (2012c), Annex 2, pp. 36–37.

36 European Commission (2012a).

37 European Commission (2012b).

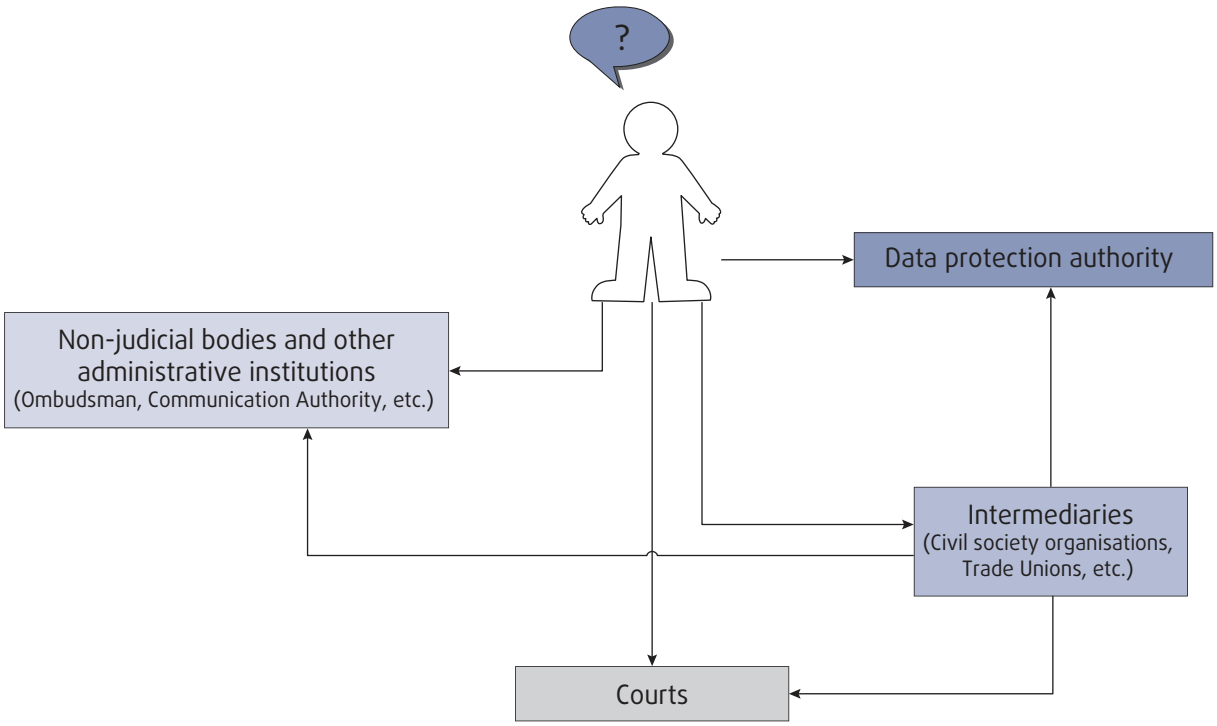
38 Explanatory Memorandum, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

2

Data protection remedies at national level

There are different ways for an individual to access remedies at national level in case of a data protection violation. The figure below and subsequent sections in this chapter illustrate the most common ones, without aiming to be comprehensive.[39] In most national systems, DPAs together with courts are the bodies most frequently involved in remedying data protection violations. In addition, there are also other non-judicial bodies and administrative institutions, such as an ombudsperson institution or a communications authority, which can offer certain types of remedies. Finally, the support and advisory role of intermediaries, in particular that of civil society organisations, throughout the whole process has also to be taken into account.[40]

Figure: Selected paths to access remedies in the area of data protection



39 See also Chapter 5 'The data subject's rights and their enforcement' in FRA and Council of Europe (2014).

40 For a similar overview of different paths to access to justice in the area of non-discrimination, see FRA (2012c).

2.1. Non-judicial bodies

Non-judicial bodies other than DPAs play a role in providing advice, guiding and taking complaints, providing a valuable addition to the statutory data protection framework.

The powers of non-judicial bodies to address data protection violations vary across the EU Member States. Often people can seek remedy via an ombudsman, such as in the Czech Republic, Italy and the Netherlands. In the Czech Republic, the ombudsman (the Public Defender of Rights) is entitled only to ask the DPA to rectify a mistake. In Italy, the ombudsman for administrative acts of municipal, provincial and regional authorities can order that access to data be denied, either temporarily or permanently. In England, the Parliamentary and Health Service Ombudsman's (PHSO's) 'Breach of Confidence' Report on the importance of data protection in breach of confidence was an illustration of the positive role of a non-judicial body in the area of data protection. Following a complaint received by the PHSO, a number of significant governmental departments have taken steps to guarantee that they cooperate and act jointly to ensure greater data protection compliance in the public sector.[41]

Other non-judicial bodies have the power to annul decisions taken by other authorities, to order rectification of violations and to grant, deny or delete information. This is the case with the Danish Press Council, which is able to delete specific information.[42] In Germany, the authority responsible for issuing permission to trade or licences to businesses can also revoke said permit or licence of a business that has violated data protection laws and therefore is not reliable.[43]

A number of bodies are also able to issue fines for data protection violations, for instance the Portuguese Communications Authority and the Italian Commission for access to administrative documents at the Office of the President of the Council of Ministers for the acts of central and national authorities,[44] the Hungarian National Media and Information Communications Authority and the Austrian Administrative Authorities. A superior authority in Latvia can demand a public or written apology, as well as order compensation in the form of both pecuniary and non-pecuniary damages.[45]

> Whereas some non-judicial bodies have sufficient powers to offer effective remedies, others are more limited.[46] Nevertheless, coordination between DPAs and these other bodies to promote data protection rights and provide more effective remedies for violations seems to be minimal. DPAs "should promote closer cooperation and synergy with other guardians of fundamental rights [...] in the emerging fundamental architecture of the EU,"[47] as the FRA 2010 report on the role of national DPAs in the EU highlighted.

2.2. Data protection authorities

The research shows that there is a variety of administrative sanctions are available across the EU Member States, including issuing an order a warning or objection, making different orders (e.g. to disclose information, to implement specific measures, to rectify, erase or block specific data, to discontinue processing operation or suspend the transfer of data to a third state), imposing fines (pecuniary sanctions), revoking licenses or reporting the matter to courts or a public prosecutor.

The Data Protection Directive sets out the powers of DPAs, granting them the ability to investigate and intervene to prevent violations.[48] Article 79 of the Draft Regulation would go further in enshrining in EU law the ability of DPAs to impose administrative sanctions. Data protection authorities often act as the first point of contact for victims of such violations, so they play an important role in remedying data protection violations. This role is often recognised by national courts, and in Finland, for instance, the prosecutors and courts are obliged to provide the DPA with an opportunity to be heard in cases under the Finnish Personal Data Act.

Whereas EU legislation, both in place and proposed, would enshrine the ability of DPAs to impose administrative sanctions on controllers, national legislation already provides a broad range of possible outcomes across the EU Member States, varying in severity. The possible outcomes range from the issuance of warnings or formal objections regarding the practices of individual controllers, to specific orders and injunctions aimed

41 PHSO (2011).

42 Denmark, Act No. 430 of 1 June 1994 on information-databases of the mass media (*Lov nr 430 af 1 Juni 1994 om massemediers informationsdatabaser*), Section 13. Failure to comply with such orders are punishable with a fine or imprisonment; see Section 16 of the act.

43 Germany, Trade Licencing Act (*Gewerbeordnung*), 1999.

44 Portugal Communications Authority (*Autoridade Nacional de Comunicações*) 2011, Supervisão e Acompanhamento De Mercado; Italy, Government (2010), p. 73.

45 Latvia (2005), Law on Compensations for Loss Caused by State Administrative Institutions (*Valsts pārvaldes iestāžu nodarīto zaudējumu atlīdzināšanas likums*), 2005.

46 FRA (2010), p. 8.

47 *Ibid.*

48 See Chapter 5 'The data subject's rights and their enforcement' in FRA and Council of Europe (2014).

at remedying the violation. As punitive measures, some DPAs also have the power to issue fines and pecuniary sanctions, or to revoke temporarily or permanently licenses necessary for the processing of information. Should the violation be serious enough, cases can also be referred to either the courts or the public prosecutor of the relevant Member State.

The extent to which these tools are utilised varies across the EU Member States. FRA data indicate that around half of the Member States empower DPAs to issue warnings or formal objections to the practices of controllers. In some Member States, allowing for the size differences between countries, these were used sparingly between 2009 and 2011; for example, in Luxembourg one warning was issued, and in Cyprus eight were issued. In Romania and Slovenia, 66 and 158 warnings respectively were issued between 2009 and 2011.

In addition to issuing warnings, in every EU Member State DPAs have the ability to issue orders or injunctions aimed at remedying certain types of data protection violations. This is in line with Article 28 of the Data Protection Directive and the proposed regulation. These measures include ordering the data controller to disclose information; to implement specific security measures; to rectify, erase or block specific data; to discontinue a processing operation; and to suspend the transfer of data to a third state.

The most common course of action taken by DPAs is issuing a fine or pecuniary sanction, as reported in 19 EU Member States. For example, the DPA in Cyprus issued fines in 20 cases between 2009 and 2011. During the same time period, the Spain's DPA issued 1715 fines, Czech Republic's DPA issued 279 fines, Estonia's issued 101, Latvia's 63, Romania's 148, Slovakia's 45, Sweden's two and the United Kingdom's nine.

The size of the fine imposed is often set out in domestic legislation, and many EU Member States distinguish between natural persons (or individuals) and legal entities (or corporate bodies). Fines can often be increased to punish recidivists, or when numerous violations have been committed. At the lower end of the scale, the DPA in Romania can issue fines up to €12,000. Fines issued by the DPA in Hungary range from €350 to €35,000, and in Greece they range from €880 to €150,000 based on the severity of the violation. In Slovakia, fines can reach €332,000. In France, the DPA can issue fines of up to €150,000 for first-time violations, and up to €300,000 if a further violation is committed within five years. At the upper end of the scale, the DPAs of the United Kingdom and Spain can issue fines of up to €500,000 and €600,000 respectively. In Slovenia, the DPA can issue fines from €2,080 up to €1,000,000 for large companies and €830 up to €20,000 for the responsible person of the company. In Poland, overall fines for not complying with a decision of DPA range from approximately €12,000 (a single-person business) to approximately €48,000 (company).

A further punitive measure employed by DPAs in several EU Member States is revoking – either temporarily or permanently – licences necessary for the processing of data. FRA data indicate that DPAs can revoke licences or authorisation to process data, but there are few recorded instances of this ability being used: six in Croatia between 2009 and 2011, and just one during the same period in Luxembourg.

In sufficiently serious cases, some DPAs can refer the case to either the courts or the public prosecutor of the relevant EU Member State.

DPAs' powers to remedy data protection violations, and the extent to which they use them, vary greatly across the EU. These powers include formal warnings, specific orders, injunctions, revocation of licences, fines, other monetary sanctions or a referral of the case to the relevant EU Member State's courts or public prosecutor. The adoption of the proposed European Commission regulation would enshrine in EU law the power of these authorities to impose administrative sanctions, namely pecuniary fines. Although the majority of DPAs already have this power, the proposed regulation would significantly increase the scope for larger fines, up to a maximum of €1,000,000, or 2 % of an enterprise's annual global turnover. For any powers to be effective, it is also important to provide necessary safeguards to ensure that they can be effectively enforced in practice.

2.3. Judicial procedures

2.3.1. Civil and administrative procedures

With regard to civil and administrative procedures, most of the EU Member States explicitly recognise the ability to award compensation in the form of damages. Several Member States report that non-pecuniary compensation can also be granted. Whereas some Member States set out in domestic legislation the amount of compensation that can be awarded, often it is left to judges to develop an accepted range of both pecuniary and non-pecuniary damages through national case law. Again, the amounts awarded vary greatly between Member States. Austria for instance, sets an upper limit of €20,000 for non-pecuniary damages, but the range of cases in other Member States suggests that awards of compensation are often much lower, ranging from €300 to €800 in Finland, up to €600 in Sweden, and from €1,200 to €12,000 in Poland.

In addition to the awarding of compensation, in Lithuania the controller responsible for the violation can be both warned and fined, from LTL 500 (approximately €145) to LTL 2,000 (approximately €580).

In much the same way that DPAs can issue orders aimed at remedying any violation, administrative and civil procedures can also result in similar orders and injunctions. In five EU Member States, courts can issue an order demanding that access be granted to specific data; 10 Member States use orders for the controller to rectify, erase or cease the processing of specific data; and in four Member States the courts are able to order that relevant third parties or the public be informed of any violation or subsequent court judgment.

2.3.2. Criminal procedures

In serious enough cases, criminal proceedings can be initiated for violations of data protection legislation. As the research demonstrates, there are a number of possible outcomes once court proceedings have been initiated: the courts can issue warnings; publicise any judgment made; prohibit an individual from managing the processing of data in the future; and compel those responsible for the violation to undertake community service.

In addition, in all EU Member States the courts can impose fines, issue prison sentences or combine both. The size of the fine or length of the prison sentence is set out in national legislation and varies between Member States. Much like the civil and administrative procedures in place, the sentence will be affected by whether the violation involves natural persons or legal entities.

In Croatia, fines imposed range from HRK 10,000 (approximately €1,131) to HRK 40,000 (approximately €5,325). In the Czech Republic, fines up to €8,500 are imposed. In the Netherlands, fines can reach €7,600 for individuals and €19,000 for legal entities, whereas, in Malta, the limit is set at €23,293. In Greece and Portugal, fines can be up to €30,000, in Hungary the amount can reach €40,000, and in Ireland individuals can be fined up to €50,000, rising to €250,000 for corporate bodies. In Latvia, fines range from €25,000 to €50,000, with Belgium setting the limit at €100,00 and Luxembourg at €125,000. In France, fines range from €15,000 to €300,000. The United Kingdom does not set a limit on the amount that a court can fine for violation of data protection laws.

In the Czech Republic, for example, the courts can order the confiscation of property; in Latvia, they can impose community service, with a maximum duration of 280 hours.

For those imprisoned, the majority of EU Member States enforce a maximum determinate sentence, most of which fall between six months (Croatia and Malta) and five years (Cyprus, France, Slovenia and Latvia). Within this range fall Belgium (two years), Estonia (one year), Finland (one year), Germany (two years), Hungary (three years), Luxembourg (one year), Poland (three years), Portugal (four years), Slovakia (three years) and Sweden (two years). In Denmark, a sentence of up to four months can be imposed. In Greece, the Court of First Instance can issue a sentence of up to three years, with the Court of Appeal able to increase this to 10 years. In Spain, the maximum sentence is seven years' imprisonment, whereas in Romania no upper limit is imposed on judges. In Ireland and the United Kingdom, no custodial sentence is applied for data protection violations.

Almost all EU Member States grant civil and administrative courts the power to award compensation, and they grant criminal courts the ability to issue sanctions in the form of fines or imprisonment. The sizes of potential fines and sentence lengths, however, vary greatly across Member States. Some respondents said the severity of sanctions makes judicial proceedings more effective. In addition to sanctions, public awareness of rights, redress mechanisms and how to take advantage of them also contributes to judicial effectiveness. The speed of decision making and the expertise of the judiciary need to be enhanced.

2.4. Intermediaries

Civil society organisations play a role in providing advice, guiding and taking complaints, providing a valuable addition to the statutory data protection framework. The fieldwork targeted intermediaries – representatives of the civil society organisations or other individual professionals that provide support for the individuals subjected to the data protection violations – and aimed to capture the opinions and experiences of those who help complainants navigate justice systems in seeking remedies in the data protection area.

When looking for potential interviewees representing the intermediaries, the fieldwork in the 16 EU Member States faced several challenges. The main problems related to the low number of civil society organisations operating in the area of data protection. Attempts to reach a set minimum number of interviewees were successful in 12 countries (Austria, the Czech Republic, Finland, France, Greece, Hungary, Italy, the Netherlands, Poland, Romania, Spain and the United Kingdom). In four countries (Bulgaria, Germany, Latvia and Portugal), researchers were able to interview fewer than six intermediaries. In most countries, it was a challenge to find representatives from organisations that specifically

dealt with data protection issues, provided support for the victims of the violations or had extensive experience in the area.

The representatives of different organisations covered by the fieldwork play an important role in bridging gaps when individuals access justice in the complex area of data protection. In the United Kingdom, for instance, civil society organisations communicate informally with governments and organisations where they have become aware of a data protection violation and informed the data controller of the problem and the significance of the issue. The intermediaries considered that the role civil society plays in providing advice, guiding and taking complaints is a valuable addition to the statutory data protection framework.

The intermediaries interviewed during the fieldwork maintained that they – or the civil society organisations they represented – mainly provided advice and information for individuals subjected to data protection violations (as noted during the fieldwork in Austria, the Czech Republic, Finland, France, Germany, Hungary, Italy, the Netherlands, Poland, Portugal, Spain, Romania and the United Kingdom). They also provide legal assistance or representation (examples mentioned by the respondents from Bulgaria, the Czech Republic, Finland, France, Greece, Hungary, Italy, the Netherlands, Portugal, Romania, Spain and the United Kingdom). The organisations provide complainants with independent advice and guidance (including legal guidance) on the remedies available, inform complainants about their rights and the procedures in detail (e.g. how to make an appeal, providing model letters), direct them to the relevant institutions or organisations and assist individuals with their complaints (and lodge complaints on an individual's behalf). They mainly offer this guidance directly (face to face), by phone or email, or through the websites of the organisations. Some of the organisations deal with data protection issues in specific areas, such as health care (or psychiatry in particular), police actions, online activities or video surveillance.

"Although very slowly, citizens are learning that there are people watching over their rights in this field."
(Intermediary, Spain)

"So we, with our partners, we give advice in various areas: legal, tax, best buy, and even in confidence, when they tell us that they have problems, we try to inform them of their rights and which legal instruments can be used by them to solve such problems. At times, instead, we take action, especially now that there is a class-action instrument, in cases where the issue can be of interest to a large number of individuals."
(Intermediary, Italy)

"The greatest priority is to inform; through the magazine and the website and media and different publications we give explanations on a lot of questions, including this one [data protection] … The second thing is that we give consultations to people who are looking for them and are interested; they get explanations about rights and procedures. After that, if necessary we refer the cases to the proper authorities […] And after that there is legal and procedural representation, where we are given the very important right to represent consumers." (Intermediary, Bulgaria)

"Our activities include providing simple advice, information and education. We involve ourselves, solicited and unsolicited, with laws and regulations and we are a point of call for people who want information on paper or digitally. This means that the direct assistance ranges from offering advice, referral, help with drafting documents, placing sample letters at your disposal to auditing and actually supporting, and being a fellow party in judicial proceedings."
(Intermediary, Netherlands)

"So, as an NGO we don't really have personnel. The activities are based on voluntary work and, as I am the vice-chairman, I try to help whenever these occur; and, in particular, because I have a legal background, I can give rather accurate recommendations. And I can tell right away if it has any chance, like if it's worth taking forward or is there some other method that could be used." (Intermediary, Finland)

"We usually give recommendations and advice to our clients, manage negotiations. If a client has problems or disagreement with the health care institution, we negotiate with it on behalf of our client. In unambiguous cases, we issue our written opinion or assessment for the legal proceedings." (Intermediary, Latvia)

Other activities of the civil society organisations mentioned by research respondents included education, research and training. For example, a French NGO runs training sessions on police files and criminal records for social workers and educators, associations and prison personnel. Similar examples were mentioned in the Netherlands and Spain. Other examples include targeted assistance to migrants in detention centres, when procedural issues have a data protection component. Respondents from several countries (Austria, France, Greece, Hungary and the Netherlands) highlighted that civil society organisations and other intermediaries raise awareness and publicise issues through media campaigns, article and publications. They monitor the situation and focus on lobbying and campaigning.

"We also have a role as public letter writer, since these people are foreigners. They are not informed of the procedure and have great difficulty understanding, and even we do not always understand. There is no notification requirement for the person who does not even know they are on file. They know that their fingerprints were taken at the time of arrest or of crossing the border, but they do not know what this will be used for, nor by whom."
(Intermediary, France)

"We issue warnings if we see new projects of authorities or private parties that are related to the privacy of internet users. We try to get media attention for these projects and we make sure that the right to privacy as laid down in the constitution is safeguarded at all times."
(Intermediary, Netherlands)

During the fieldwork, the intermediaries highlighted problems related to access to resources. Having limited resources, the NGOs are not able to take up cases and work to the extent that they want to. For example, the respondents from Romania maintained that for lack of resources they could not offer the services of a permanent specialised legal counselling unit, although each of them provided some legal assistance according to the resources available to them. The respondents from Bulgaria said that they were not able to file class actions, as the NGOs have to prove that they have enough financial resources and the ability to cover the expenses of the proceedings. According to the interviewees, very often NGOs were unable to give this assurance and cover the costs. This keeps them from using this legal mechanism.

Some representatives of civil society organisations in the Netherlands mentioned that they offer occasional support and advice to individuals and operate selectively because they have limited means. This is particularly the case when launching lawsuits.

The intermediaries interviewed in all the 16 countries identified the need to improve awareness and provide information to the general public, victims of violations and public authorities on privacy and data protection issues. Also, some of the respondents indicated the need for greater cooperation and coordination with other agents in the area of data protection, including public institutions and civil society organisations.

"We would recommend better collaboration with associations, which are those that really represent citizens."
(Intermediary, Spain)

Italian intermediaries also recommended giving greater consideration to the effectiveness of the existing legislation because the continuing technological advancement is so fast that five-year-old legislation could already be obsolete. At the same time, they emphasised the need to raise awareness of issues of data protection. They noted that awareness about privacy issues should be a priority because it allows for a better understanding of what kind of protection there is for individuals.

Intermediary organisations emerged in the fieldwork as an important source of information, advice, legal assistance and representation. They also create awareness and publicise data protection issues and possible remedies. However, the fieldwork shows that there is a scarcity of civil society organisations that are able to offer comprehensive and well-publicised services, developing a public profile in the area of data protection. This limits people's access to remedies in practice.

FRA opinion

The report highlights the importance of intermediary organisations as a source of information, advice, legal assistance and representation. However, only a very limited number of civil society organisations are able to offer comprehensive services for victims of data protection violations. The EU and its Member States should increase funding for civil society organisations and independent bodies in a position to assist such victims seeking redress.

3 Accessing remedies in the area of data protection: experiences of individuals

This chapter focuses on the experiences of the individuals subjected to data protection violations who have sought or have considered seeking remedies. During the interviews, the complainants and non-complainants were asked to provide details about the data protection violations they had suffered, the factors which led them to decide to seek remedy, how they perceive the damage caused, how they found out about the violations, and how they chose a specific remedy or decided not to seek redress. The following developments present the fieldwork findings and an assessment by various actors of their experience when seeking remedies.

3.1. Data protection violations faced

The individuals subjected to the data protection violations were asked about the violations that led them to seek redress. The results from the fieldwork covered a wide and diverse range of types and areas of the data protection violations faced by the research participants in the last three years before the research in all the 16 EU Member States.

The most frequent data protection violations that were mentioned related to internet-based activities. These included social media, online shopping, leakage of personal data from e-shops, hacking of email accounts and databases, identity theft, security breaches and misuse of personal data by global internet companies. Internet-based activities clearly emerged as a high-risk territory for data protection. For example, one Finnish judge remarked that it is good that there is a special unit of police that has the ability to investigate computer crimes very thoroughly if there is need to do so. The 2011 Special Eurobarometer survey indicated that 43 % of internet users said they had been asked for more personal information than necessary when attempting to access or use an online service.[49] The 2012 Sepcial Eurobarometer survey on cyber security[50] showed that, when using the internet for online banking or shopping, Europeans had two main concerns such as someone taking or misusing personal data (mentioned by 40 % of internet users in the EU) and security of online payments (38 %). Also, security concerns influenced the behaviour of internet users, as 37 % of the survey respondents said they were less likely to give personal information on websites.

Another common data violation was direct marketing and commercial prospecting without the consent of the recipient, when the personal data were misused on mobile phones, by email or by post. The fieldwork suggests that mobile operators and debt collectors are often responsible for these violations. Irregular practices such as selling personal data to third parties were noted.

The interviewees often referred to video surveillance (in particular, no signs warning about the surveillance) at the workplace, in the public spaces or in

49 European Commission (2011). The survey was conducted in the EU27 between the end of November and mid-December 2010. A total of 26,574 Europeans aged 15 and over were interviewed. All interviews were conducted face to face in people's homes and in the appropriate national languages.

50 European Commission (2012d). The survey was conducted in the EU27 in March 2012. A total of 26,593 Europeans aged 15 and over were interviewed. All interviews were conducted face to face in people's homes and in the appropriate national languages.

supermarkets. Several individuals in different countries had also experienced secret surveillance conducted by public authorities with special technology or by secretly installed CCTV.For example, it is worth mentioning that several DPAs had detailed guidelines regarding the use of CCTV (for example, the United Kingdom).

In workplaces not affected by video surveillance issues, interviewees alleged other violations in employer–employee relationships. These included the collection of employees' personal data, access to personal data stored in employers' computers, use of badging and global positioning systems, discriminatory use of sensitive personal data collected through surveys or audits, and disclosure of employees' data by employers.

According to the fieldwork results, financial violations were also quite common, including breaking into bank accounts and similar security breaches, such as credit card hacking.

Most of the violations faced by research participants were related to the processing of personal data, such as collection, storage, disclosure and dissemination, for example:

- Unjustified transfer of personal data from data controllers (employers, public authorities, mobile operators, credit institutions, etc.) to third parties. In this context, it is worth mentioning the unauthorised transfer of data to debt collection companies by credit institutions and selling databases with contact details of persons by commercial companies. Furthermore, the German fieldwork highlighted that, in five cases, parents blamed child care institutions or youth welfare offices for unjustified transfer of personal data to other parties.
- Improper and excessive collection and storage of personal data by secret services, the police or public authorities, or by supermarket chains, without legitimate purpose, proportionality and sufficient guarantees of security.
- Storage of inaccurate or unnecessary information.
- Manipulation of inaccurate personal data stored and processed legally.
- Unlawful disclosure of personal data to unauthorised persons.
- Unlawful disclosure by the justice system of confidential personal data related to domestic violence during a criminal case and divorce proceedings.
- Publication of personal data in the media or on the internet.
- Publication of personal data of parties in proceedings in the legal databases or on the intranet in courts' databases.

The intermediaries and practising lawyers in Greece raised a case in which, shortly before the 2012 election, the Greek police took some sex workers into custody. The authorities performed rapid HIV testing on them, diagnosed them HIV positive and charged them, and their names, photographs and personal details were published on the police website.[51]

The other data protection violations mentioned were connected to the rights of the data subject, especially with his or her right of access:

- refusals of access to personal data held by the police, medical services, social services, employers and others or insufficient responses to requests for access to personal data;
- refusals to correct, delete and block information in personal data files (such as law enforcement, health sector))or insufficient responses to requests for corrections, deletion and blocking of information in personal data files.

Public authorities (national and local governments, and law enforcement authorities) and private entities (e.g. media companies and financial institutions) alike were alleged to have violated data protection.

Healthcare institutions were highlighted as having the potential to infringe a person's privacy in different ways, such as illegal access to medical data by third parties or denial of the right of access by data controllers. The fieldwork also indicated other types and areas of potential violations such as in education, social security, housing, political participation and detention, census, public transport, the energy sector, the legal sector, immigration and asylum.

Interviewees mentioned the following cases in relation to personal documents: forgery of personal documents and their use to obtain financial profit or other gain; photocopying ID cards; or requesting an ID card to access a building or to complete contracts or high-value purchases.

When asked how the subjects of the data protection violations found out that their rights had been violated, a variety of ways were mentioned. Either the interviewees noticed directly unlawful activities as a consequence of a violation of privacy ('on the spot') or they encountered a variety of problems in their daily lives arising from the unlawful activities.

51 European Centre for Disease Prevention and Control (ECDC) (2013).

Among the unlawful activities they identified, the interviewees listed the following experiences most often: noticing unregistered cameras, becoming an addressee of direct marketing and soliciting messages, spam emails, being blocked from normal activities such as signing into email accounts, reading their names in print or online articles and similar occurrences.

"Q. So the camera was mounted there to supposedly film the scanner clock. How did you perceive that there had been a breach?"

"A. As soon as we knew that they'd put up a camera, I always wanted to know exactly what they were filming, didn't I? Because we all know that cameras swivel around in a wide angle and some cameras have a fully circular coverage. [...] Why doesn't he let us see what he's filming? [...] I asked a co-worker to go to the vicinity of the washroom, and, as my door was open because the cleaner was coming in, I stood there watching the picture on the screen. I asked my co-worker to stay there to see if the camera caught him or not. And of course, after I had told him: 'OK, go in and come out of the washroom', I saw the lad go in and come out on the screen. I saw it all."
(Complainant, Portugal)

In Finland, nearly half of the complainants interviewed said that they became aware of a data violation when they received unwanted direct marketing messages. At the time, they were aware that direct marketing without the recipient's consent is unlawful. Such violations were also mentioned by the interviewees from Bulgaria, the Czech Republic, France, Hungary, Spain and the United Kingdom.

Fieldwork indicated that some people found out about the data protection violations when they faced financial problems, or problems at banks and/or other similar institutions, when a person was contacted by a debt collection company and was asked to pay a debt that he or she was not responsible for (the Czech Republic, France and Hungary).

The complainants also realised that they were facing a data protection violation when they encountered employment problems, such as when they received an unfavourable decision from their employer or were denied access to jobs (noted in Bulgaria, France and Poland). In these cases, the interviewees linked the fact of being fired from their jobs to the data protection violation that they had experienced.

Data protection violations were discovered in a number of other ways. Some reported that they discovered the violation before they had noticed any consequences. Others discovered the violation only as a result of the consequences arising from it (noted in Austria, the Czech Republic, Finland, France, Germany and Romania).

Others discovered a violation when they exercised their right to access data. This was reported in the Netherlands, where three complainants discovered that care instituions for young people or healthcare institutions held incorrect or irrelevant data and that this data had beentransferred to third persons or institutions. Complainants in Germany highlighted eight cases where they had exercised their right of access to information and discovered illegally stored or false personal information, or a public procedure register (*Verfahrensverzeichnis*) that they considered to be flawed.

Less common ways in which people found out about data protection violations were through awareness-raising articles or activities (e.g. Austria, Latvia), or by being told about the disclosure of personal data or learning of it from a third party (the Netherlands and the United Kingdom). Some of the complainants found out by consulting experienced professionals such as lawyers (Latvia and Portugal). Fieldwork in Portugal highlighted that this was particularly the case where identity theft and internet-based violations were concerned.

"One morning a lady called me, I even know her name, and very strongly demanded an interview with me in which she would ask questions and I would answer them. As I am not fond of anonymous phone calls, I asked her to tell me her name, so she introduced herself and told me she was conducting a research about banks and obtained my personal information from my bank, [name]. She went on to tell me my personal ID number, address, mobile phone and I even think she knew the form in which my account was set up in [bank name]. In short, she knew everything."
(Complainant, Czech Republic)

"Q. How did you find out that your name had indeed leaked out and been mentioned?"

"A. My neighbour said to me: 'Good morning [name], are you off for another nice day of defrauding?' I thought he was cracking a joke. I thought 'what is this man talking about?' And then I found out that they had published something about me in [name of magazine]. Then I was at the physiotherapist's and I while was waiting I saw my name in the [name of magazine]." (Complainant, Netherlands)

"Q. How did you find out that you had to provide your fingerprints and that you thought'I don't want that'?"

"A. I read it on the news, on the internet. I thus ended up at that foundation [NGO name], again and again and then I read on their website that they are against the Passport Act. Finally, I registered myself as a volunteer and later I was asked if I wanted to become a co-plaintiff."
(Complainant, Netherlands)

The research reveals that having an understanding of what constitutes a data protection violation, and of the laws surrounding data protection, better equips citizens to identify when they themselves have been the victim of such a violation (as reported in Austria, Germany, Hungary, Latvia and Portugal). From the initial stage

of finding out about a violation to the stage of seeking redress, knowledge empowers people to take appropriate steps to protect their rights.

Internet-based activities, direct marketing and video surveillance through the secret use of CCTV emerged in the fieldwork as the most frequent sources of data protection violations. A significant proportion of data protection violations in the EU takes place on the internet. Government bodies, law enforcement agencies, and financial and health institutions are most often responsible for these violations. Awareness is a crucial prerequisite to ensure that individuals can identify a data protection violation and initiate a remedy.

3.2. Damage caused by a data protection violation

When asked about the damage caused by the data protection violation, the complainants and non-complainants most commonly tended to describe it in psychological or social terms. In the former case, they focused on their emotions; in the latter, on the opinion of other people or the impact on their relations with other people. They mentioned varying degrees of emotional distress, offence, insecurity (including feelings of being persecuted or under surveillance), helplessness or damage to their professional or personal reputation, loss of trust and other forms of moral damage (in, for example, Austria, Bulgaria, Germany, Greece, Hungary, Italy, Latvia, the Netherlands, Poland and Spain). A complainant in Spain noted that an aspect of this is feeling "impotence regarding an abuse of power".

"Simply the uncertainty – not knowing, even who has this data, and how it's been used – is the damage. There might be other more particular damages but I don't know about them. And of course that's why access is so important. Why accounting for the use and disclosure of information is so important. Without that, one cannot know what other problems there may be, or what damage may have been done." (Complainant, France)

"I left [my job] on very painful terms. […] My heart was aching […] and I couldn't defend myself because I didn't know whether these accusations existed." (Complainant, Greece)

"The consequences [of the violation of medical secrecy] were dire. All the people I trusted broke away – parents, caretaker, doctor. At stake was the loss of my self-determination […] My whole world collapsed, and I was left alone without money and support." (Non-complainant, Germany)

"It was only the bother it caused me at a personal level. There was no material damage. I didn't want to go on receiving material from the publishers […]" (Complainant, Portugal)

While describing the impact of the experienced data violation, the overwhelming majority of interviewees mentioned such things as disturbance of daily life, defamation, disappointment due to misplaced confidence, shock, fear, feeling of injustice, humiliation, a sense of dispossession or lack of control over their own data.

In most of the 16 EU Member States, few complainants have suffered financial losses as a result of their data protection violation. Financial damage, although reported less frequently, included refusal of access to credit, financial losses through the unlawful assumption of responsibilities and financial losses due to identity theft. In many of those cases, respondents describe the financial loss as minor, that is, the financial sums were not large. Most of these cases related to telephone calls, postage and the costs of having records accessed and amended.

"Q. Regarding the damage this situation has caused you, were there various kinds of damages?"

"A. You won't believe it. My life took a turn of 180 degrees. I can't manage to get on with my life. I can't manage to do what I wanted to do. I have projects to accomplish in life, I have plans, ideas […] But I can't do anything. I can't because I'm a persona non grata at the banks and similar institutions. Or rather, my name doesn't count." (Non-complainant, Portugal)

Interviewees in the Czech Republic, Italy, the Netherlands, Portugal and Romania noted that violations in the area of employment had caused damage such as disciplinary proceedings, suspension and/or termination of employment or risk of dismissal. In some of these cases, the damages relate to economic (financial) losses (as mentioned in the fieldwork in Italy, the Netherlands and Portugal), including missing out on job opportunities, not being able to get a loan, not being entitled to health care or benefits, high cost of legal representation, or immediate financial losses and the prospect of financial losses through the unlawful assumption of responsibilities.

Most of the interviewees in the 16 EU Member States covered accessed remedy in cases where the damages caused by the data protection violation were defined mainly in psychological terms. The research observed few exceptions where the interviewees said they did not experience any damage.

Complainants and non-complainants interviewed in the research describe the damage from data protection violations as psychological and social in nature, such as emotional distress or reputational damage. Participants also, although less frequently, report financial damages.

3.3. Reasons for seeking remedy

Participants were asked what reasons made them seek remedy after an alleged data protection violation, or what encouraged the intermediaries to support their cases. The interviewees named different reasons for seeking redress that also reflect their preferred outcomes for the procedures. Most of the respondents were concerned about prevention of violations to protect others in future, recognition of violation, termination of the violation or a favourable change in their situation. The financial compensation was not a prevalent reason for seeking redress.

Some of the respondents were motivated to seek redress mainly by their personal considerations and situations. They wanted to remedy a situation that relates solely to the individual seeking the remedy, because of the personal impact the violation has had on him or her. In this case, the interviewees' answers commonly feature issues such as "fixing an unjust situation", "correcting damage to identity or image", "clarifying wrong records", "rectification/deletion of personal data", "achieving rehabilitation", "imposing sanctions against violators" and "stopping the abuse of power and excessive unlawful control by employers".

A much greater share of respondents wanted to minimise a possible risk of other individuals becoming a victim of data protection violations. They most commonly mentioned "prevention of future violations of rights", "awareness raising", "stopping the wrong practice", "standing up for fundamental rights", "teaching a lesson to concerned authorities", "obtaining an acknowledgement of the violation from a competent authority" or "imposing a sanction on the perpetrator". These reasons motivate intermediaries (NGO activists, representatives of the civic organisations) and lawyers to take up such cases.

"I think that leaks of personal data must be addressed and scrutinised. Someone must be able to tell the bank what it can or cannot do." (Complainant, Czech Republic)

"At that moment, I did not think of redress or compensation. I was dissatisfied [...] that if an enterprise has received your data, it believes it can do anything with them. I wanted to suspend such a practice. I wanted my data to be deleted." (Complainant, Latvia)

"Our main motivation was to fight the violation of fundamental rights and freedoms which are enshrined in the Constitution." (Complainant, Portugal)

"It was an overall control over people. [...] One of the reasons was that, among others. The times people went to the toilet, every time people left their workplace, they knew. All that led to a bad working environment." (Complainant, Portugal)

"I think the only remedy I could see as encouraging is [having it] acknowledged that they were aggrieved or receiving a decision saying 'what happened to you was not ok, your rights have been breached'." (Intermediary, Romania)

"Factors that play role in building the confidence to take the case are that a person's patience is exhausted or emotional harm suffered has been severe [...]" (Intermediary, Latvia)

"I would like to see the business, [company name] for example, take a moment to reflect and say 'hmm, we are doing this wrong, let's change it' but it's not what they want to do." (Complainant, Czech Republic)

"Q: Why did you decide to take a legal path?"

"A: Because I felt that my rights were violated. My philosophy in life is that, when somebody violates my rights, I can't agree to that, especially when I see the chance of success." (Complainant, Poland)

"I am by nature a defender of civil liberties and rights. I hate police files, especially when there is no consent and especially when it is excessive. They take my data and the least thing would be to know what they are going to do with the data and what the redress mechanisms are." (Complainant, France)

"It [stored data] can be used against me, be manipulated. Then we will end up with a dictatorship." (Complainant, Netherlands)

"I was not aware of the accusations, this file was like a threatening box, a box that included names and accusations and that sent thunderbolts against me. [...] Thus, I said that at least I should know what is in this famous file, this nuclear warhead that sent poisonous darts towards me without me knowing." (Complainant, Greece)

"My passwords of my Yahoo, Gmail and Facebook accounts were stolen and this person assumed my identity for more or less a year. He sent emails in my name and made my Facebook profile that had my picture in it and all my contact addresses; the Facebook contents were made to be very, very obscene. It was therefore very defamatory and extremely humiliating, and basically it was this. [...] Obviously, the first thing is getting to learn who the one is behind it all, isn't it? To stop it. I wanted it to stop, didn't I?" (Complainant, Portugal)

To some extent, the decision to seek remedy might be related to concerns that damage may arise from the violation. In some of the cases where no direct personal harm (e.g. financial loss) was experienced, the individuals tended to refrain from seeking remedy.

"Well, it would be at the point when I feared something terrible would happen. If I was robbed based on the fact that I raised my insurance coverage, I think then I would take this step. At the point when these are just my fears or hypotheses, I say to myself that it's not necessary to worry and that it really doesn't bother me that much." (Non-complainant, Latvia)

Many complainants accessed redress mechanisms on the basis of psychological or social damage. Possible compensation was not a prevalent reason for seeking redress.[52] Some respondents from Finland, Germany, the Netherlands, Poland and the United Kingdom mentioned that they had sought monetary redress; however, in most cases financial compensation was not a driving motivation and it was rarely sought.

"For me that would have been more than enough. Compensation? No. Not even from a moral perspective. I would have been happy with just having someone who establishes that a breach happened." (Complainant, Hungary)

The non-complainants and other interviewees were asked what had prevented the subjects of the violations from seeking a remedy or from initiating any procedure. The reasons differed according to the situations and contexts in which the violations were faced, but the most commonly mentioned motives are discussed below. Issues related directly to the procedure (duration, estimated costs, gathering evidence) are partly covered in the next section, on the choice of remedies. Lack of information or knowledge significantly contributed to some individuals' decisions not to exercise their rights, as the report discusses later. Specific personal and other reasons that made individuals uneasy about initiating the procedures are also discussed.

Many respondents from different countries said they lacked trust in the effectiveness of the remedies in the area of data protection or in public institutions in general. Examples are provided by the respondents from Bulgaria, the Czech Republic, France, Germany, Greece, the Netherlands and Romania. In several of the 16 EU Member States studied (e.g. Austria, France, Germany, Latvia, the Netherlands), doubts over the chances of success or satisfactory outcomes stopped the non-complainants initiating the redress procedure.

Among their other reasons, many of the non-complainants and interviewees from the other target groups referred to fear of consequences or certain 'sanctions', retribution or victimisation if the remedy were sought. In most of these cases, being a dependant influenced the decision of the individuals subjected to the data protection violations, as they were afraid to lose their job, face revenge from an employer or suffer other forms of harassment on a regular basis. The interviews in Austria, Bulgaria, the Czech Republic, Finland, France, Germany, Greece, Hungary, Italy, Latvia, the Netherlands, Poland and Romania provided evidence of this. For example, in the cases of cyber-bullying, people were afraid of making the situation worse.

"People are afraid of being harassed. Someone is afraid to lose their job, someone is afraid because of the employer. People choose things which are the most important for them; sometimes it is just a question of fear." (Lawyer, Poland)

"The problem of dissuasion is primarily in the context of employment, there are fears of reprisals. The fear is of losing one's job. Whether in a small or large company, it is easy to find the person behind the complaint. This does not prevent the increase in number but it is still an obstacle." (DPA staff, France)

"For cyber-bullying, often people are afraid of worsening the situation and prefer to try to resolve it by themselves, before making a complaint" (DPA staff, France)

Some of the interviewees said that they refused to complain in order to forget the situation and avoid emotional burden (e.g. non-complainants from Greece and the Netherlands). Others mentioned that no actual damage was experienced, or that any impact on the person's rights and interests was insignificant (non-complainants from Bulgaria, Spain and the United Kingdom).

"For some people, the best protection is silence." (Intermediary, Greece)

"When you have a job interview and you are asked tons of questions, or when you apply for credit, the employer or banks go too far in their questions, which is totally unlawful; except that, as you need this job or this credit, you will not do anything. You're not going to seek redress either, because you know that they will 'grill' you at the bank or company." (Lawyer, France)

Some of the non-complainants were uneasy about exercising their rights because they perceived the perpetrator being too powerful. The respondents spoke of powerful 'others' such as bank, hospital, mobile phone provider, etc. This was expressed by several respondents (e.g. in Greece, Hungary and France). Also, some of the non-complainants felt that the offences were considered so common that their social environment was not supportive and did not consider them to be real violations (as noted in Greece regarding the calls from mobile operators and debt collectors). Another quite distinct opinion mentioned by a few respondents related to their fear of being stigmatised and considered paranoid for raising issues related to the data protection violation.

"People are afraid of complaining about their doctors because they are concerned about who will further treat them; they also do not choose to complain of a particular health care institution if it is the only one of this kind in the country." (Intermediary, Latvia)

52 In seeking compensation, complainants would have to initiate court proceedings. The additional time and costs involved in court proceedings could be a factor in dissuading complainants from seeking this form of remedy.

The interviewees also expressed their concerns about anonymity and confidentiality, fearful that the remedy procedure would require them to disclose their private issues (e.g. respondents from Italy and Romania), or would result in even 'more data' being stored or compiled (France). One of the ways in which this particular barrier can be overcome is by being able to make anonymous complaints. Representatives from NGOs and lawyers in the Netherlands emphasised that it would help individuals come forward if they could file a complaint about a data protection violation anonymously, particularly if it was against an employer or an organisation on which they depend financially or in any other way. Some lawyers also suggested that an anonymous 'hotline' for employees be created to file a complaint against employers who violate their rights.

"I think it'd be good if one was able to make an anonymous complaint or in that sense complain, where the employer doesn't realise who in the company filed it, I think it'd be good if such things were taken seriously at the relevant centres because I don't think they are. […] Through anonymity that would be safe, I mean I understand that not every anonymous complaint can be dealt with in detail, because then they'd act as some kind of instrument of denunciation, but if that were to happen in large numbers in a company." (Non-complainant, Austria)

The mechanism of *ex officio* investigations conducted by the national DPAs offer another possibility, as respondents in Bulgaria, Italy and Romania suggested. A Romanian lawyer explains it in this way:

"Theoretically, when filing a complaint, you must indicate the perpetrator, the subject you are complaining about, which in this case is the data processor. But there is another way, and this is why specialised assistance and support are required: the Romanian DPA carries out inspections and verifications upon request (based on complaints), but also ex officio. Thus, if a complaint does not fulfil all procedural conditions, but the situation indicated in its content is one that poses problems from a data protection perspective, the authority will proceed to conduct an investigation upon self-referral, ex officio." (Lawyer, Romania)

While discussing possibilities to increase accessibility and efficiency of the remedies in the data protection area, interviewees mentioned broadening the legal standing rules, such as through collective redress.[53]

Suggestions for a class action type of procedures were raised by the intermediaries and legal professionals from most of the EU Member States covered by the fieldwork (e.g. Austria, Bulgaria, the Czech Republic, France, Germany, Greece, Hungary, the Netherlands, Romania and the United Kingdom). The main arguments for class action are related to the correction of power relations in the proceedings and possible reduction of costs for the individuals subjected to the data protection violations.

"Whether I fight for this alone or whether this is done by 50,000 people makes a big, big difference."
(Intermediary, Germany)

According to the respondents from France (from the intermediaries' point of view) and Greece (from the lawyers' point of view), in the absence of class action procedures, the issue of costs, along with other problems, is particularly offputting in sectors such as commerce/consumers. However, the fieldwork suggested that, in order to make this procedure accessible, changes in legislation are needed. For example, currently in Bulgaria the law requires plaintiffs (in most cases NGOs) to prove that they possess sufficient financial resources to cover the expenses of the proceedings. However, often NGOs are unable to do so. These problems were observed in other countries as well.

"So looking at the argument in favour of class actions and collective redress? From our perspective, I think it is so well suited for data protection, because it tends to be huge numbers of people which are affected. The costs of, individually, taking a company to court for redress far outweigh the costs and so it makes sense for people to pull together and to get a nominated organisation to take the heat out of it. […] [We want a system] that would mean that a nominated organisation, someone like a consumer's organisation, should be able to take an action on behalf of all those individuals that have been affected and anything that wasn't claimed by the victim should be poured back into charitable purposes." (Intermediary, United Kingdom)

In its recent Recommendation of 11 June 2013,[54] the European Commission specifically refers to the area of data protection as the field "where the supplementary private enforcement of rights granted under EU law in the form of collective redress is of value". The current draft reform package provides organisations or associations with the right to lodge a complaint on behalf of one or more data subjects before relevant courts or before a supervisory authority. In this respect, the FRA Opinion on the proposed data protection reform package can be reiterated:

53 FRA (2011a), p. 39; FRA (2012), pp. 41–42; and FRA (2012b) pp. 28–29.

54 European Commission (2013b), pp. 60–65; see also European Commission Communication *Towards a European horizontal framework for collective redress* (2013c).

"Insertion of the right of any body, organisation or association in the draft proposals to lodge a complaint regarding breaches of the protection of personal data – acting in the public interest rather than only on an individual's behalf – could be contemplated. Such an amendment would enable civil society organisations and other bodies working in the data protection field, and having the necessary expertise and knowledge of the legal rules and situation in practice, to take a more direct role in litigation. This would in turn help to ensure better implementation of the data protection law, in particular where certain practices affect a multitude of individuals and/or where the victims of a breach of data protection rules are unlikely to bring individual actions against a data controller, given the costs, delays and burdens they would be exposed to. The introduction of broader legal standing rules would have to be done hand in hand with specific safeguards to preserve the fine balance between preventing abusive litigation and effective access to justice for data subjects."

Those who had experienced data protection violations seek redress for many reasons, such as rectification or deletion of personal data or sanctions against violators, the fieldwork showed. Respondents say they seek to protect others by preventing future violations and to gain recognition that a violation had taken place. However, various considerations tended to dissuade those who had experienced data protection violations from lodging complaints. These include lack of trust in the remedies and authorities, fear of negative consequences, retribution or stigmatisation, or perceptions that the perpetrator was too powerful. Those interviewed suggested that one specific way to increase accessibility and efficiency of the remedies in the data protection area is to further broaden the legal standing rules.

3.4. Choice of remedy mechanism

Whereas Chapter 2 above details the remedies available and the possible outcomes arising from each, this section looks at information from complainants and non-complainants on what redress procedures they used or considering using. The fieldwork suggests that the majority of the complainants in the 16 EU Member States covered during the research lodged a complaint with the national DPA (or, in Germany, at the federal DPA and the state DPAs).

The redress mechanisms operated by the courts were used less frequently than those operated by DPAs, and fieldwork results indicated that few victims of data protection violations approached the courts (the fieldwork recorded interviewees' experience in judicial proceedings in Austria, Bulgaria, the Czech Republic, Finland, France, the Netherlands, Poland, Romania and the United Kingdom). When utilised, civil procedures were used more frequently than administrative and criminal proceedings. Finland might be mentioned as an exception, as most of the interviewees there (judges and legal representatives) could not recall any civil cases during their careers. They reckoned that data protection issues were not pursued as civil matters in Finland because the risk of expenses was simply too high for the complainants. It can be concluded that, in Finland, the data protection violations are dealt with in criminal courts or by different means of mediation, but individuals do not generally take their cases to civil court.

FRA opinions

Victims are often reluctant to bring claims. Allowing civil society organisations to bring claims to court or conduct investigations could constitute an important step to help enforcement. As already emphasised in other FRA reports and opinions and confirmed by the findings of this report, strict rules relating to legal standing prevent civil society organisations from taking a more direct role in litigation in cases of fundamental rights violations (see the 2011 FRA report Access to justice in Europe: an overview of challenges and opportunities *and the 2012 FRA report* Access to justice in cases of discrimination in the EU: steps to further equality).

The 2012 FRA Opinion on the proposed data protection reform package *in particular says that the EU should consider further relaxing legal standing rules to enable organisations acting in the public interest to lodge a data protection complaint where victims are unlikely to bring actions against a data controller, given the costs, stigma and other burdens they could be exposed to. As underlined in FRA reports on access to justice, this would also ensure that cases of strategic importance are processed, thus enhancing the culture of compliance with data protection legislation. Such broadening of the legal standing rules should be accompanied by additional safeguards preserving the right balance between the effective access to remedies and abusive litigation.*

"The judicial system, particularly the traditional areas of civil law and criminal law [...], has only just begun to show developments concerning data protection. The [data protection] law has been in force for two or three years. It remains to be seen what the criminal prosecution authorities will make of the data protection law. As far as I am aware, there has only been one case in criminal law. In civil law, it is a similar situation; however, there are fortunately already several cases [decided] by the Supreme Court in the area of data protection. Apart from those cases, the data protection law hardly plays a role in everyday legal practice." (Lawyer, Austria)

Other options taken by the research participants included filing a complaint for disclosure at the ministry of the interior, filing a police report, contacting the public prosecutor's office and turning to other national or local authorities. Examples of such authorities are a local governmental family care service, a national authority for consumer protection, a national media and information-communication authority, the press council or an authority working conditions.

Different reasons and factors influenced the choice of remedy mentioned by the interviewees during the fieldwork. Most complainants, non-complainants and representatives of the national DPAs mentioned the same arguments for the choice.

There was not much choice in seeking redress in the case of the data protection violations: most interviewees identified the national DPAs as providing the only procedure available to tackle the data protection violation. Others considered DPAs to be the appropriate mechanism(s) (as mentioned by interviewees from Austria, Bulgaria, the Czech Republic and the United Kingdom). Other motives for choosing a specific procedure were related to cost-effectiveness (procedures available free of charge), short duration, the relative simplicity of the procedure and the fact that there is no obligation to acquire professional legal support. Some of the interviewees received advice from some institutions or lawyers before deciding on a specific procedure. The decision of which procedure to select is closely related to knowledge and awareness of the issues.

Decisions were also made on the basis that the violations committed fitted the mandate of the institution or its competence (as mentioned by interviewees from Finland, France, Germany, Latvia and Portugal). The public profile of the DPAs and their recognised expertise in the area were also given as reasons for the choice of redress mechanism.

"I could only see the data protection authority [as appropriate] [...] It was what I thought was the most official. Perhaps also the least aggressive. Because of course one can always resort to legal counsel, we can always resort to other means." (Complainant, France)

"Because this is the Portuguese Data Protection Authority's job. And even if we went to the Authority for Working Conditions (ACT), it would forward these issues on to the Portuguese Data Protection Authority." (Complainant, Portugal)

"[If] you go to the court without appealing to the DPA, the court could say that the extrajudicial examination procedures were not passed." (Complainant, Latvia)

"Well, basically it was the only possibility for me because I was not in the position financially to take counsel with a lawyer to inform myself what else would have been possible. So there is just this relatively harmless measure of filing a complaint at the Data Protection Commission." (Non-complainant, Austria)

"You know, I'm 76 years old, I'm not used to this. I've never taken legal action. For legal action you need a lawyer, you have to do this, do that... But if there are large sums of money at stake, yes." (Complainant, France)

"The complainants apply to the DSI [Latvian DPA] if there is a problem which could be resolved only by the DSI. Of course, a person can go to the court, but this will take longer time and more money." (DPA staff, Latvia)

Participants drew attention to the fact that, in many of the countries they were living in, there were no branches or offices of the DPAs which would facilitate access for people who cannot afford the high cost of travel.

The cost and length of proceedings were also issues that weighed on the minds of complainants and potential complainants. Applying to a national DPA was also perceived as a way of avoiding the costs, lengthy proceedings and need for a lawyer that were deemed inevitable if court proceedings were commenced (with fieldwork suggesting this was a concern in Austria, Bulgaria, Hungary, Italy, Latvia the Netherlands and Spain).

"The Polish law and justice system is very inefficient and operates partly to exhaust the interested parties, to wear them out. So, there was a moment when, let's say I got angry a bit, that's when I reported this crime to the prosecution service, but later all these things started to wear me out. Unfortunately, I must say, these procedures take so long. In this case it happened quickly anyway, because in the end the decision was given after a year and five days after the perpetrator had committed the offence. It is quite fast, according to the Polish standards. Still, I generally think it's very long." (Complainant, Poland)

"Complainants are in favour of doing everything that it is possible to do (to lodge a penal or a civil lawsuit, to ask for an indemnity, to address the Supreme Court) provided that there are no costs attached." (Lawyer, Spain)

Some of the complainants said that the procedures chosen were the only ones they knew. For example, a complainant from Finland mentioned the police, and a complainant from Spain mentioned the national DPA. Others had chosen them because of previous negative

experiences with, for instance, the court (for example, a complainant in Hungary chose a national DPA for this reason).

The choice of redress mechanisms depended to a large degree also on the advice received and information available. However, a significant proportion of the complainants interviewed in many of the countries said that they themselves had taken the decision to seek redress (e.g. in the Netherlands one in three, in Finland over half, in the United Kingdom the great majority of the complainants). The fieldwork results indicate that civil society organisations, lawyers and public bodies such as national DPAs, as well as informal channels including family members and friends, provided advice about redress mechanisms in practice. Also, the internet in general, specific websites, TV and newspapers provided basic information about available redress mechanisms for the complainants and non-complainants interviewed.

The most commonly indicated sources of specific mechanisms for redress were advice from lawyers and NGOs; interviewees from Austria, Bulgaria, the Czech Republic, Finland, France, Germany, Greece, Hungary, Latvia, the Netherlands, Poland and Portugal mentioned these sources. In some countries, fieldwork suggests that lawyers played less of a role. Interviewees attribute this to their alleged lack of expertise in this area, to a lack of access to lawyers (as mentioned by the interviewees from Hungary and Portugal) or to the relatively high costs of obtaining legal advice (Poland).

The subjects of the data protection violations perceived the national DPAs to be the primary public bodies that provided advice in person, through official websites or by phone. As a representative of the German DPA put it, many potential complainants "do first call to check whether they are at the right place." Also, the national DPAs advised on the other options available. For instance, a few Finnish complainants said that the DPA advised them to file a police report because the complainants wanted the offender to be caught and punished.

Different organisations and bodies were mentioned during fieldwork. These play a role in providing advice on the redress mechanism chosen. For example, in Germany the focus groups with both intermediaries and DPA staff described the data protection officers of public authorities and private companies as important contact persons. The following are mentioned as illustrations of possible intermediaries: data protection officers in the workplace (Austria, Finland), workers' representatives or trade unions (the Netherlands, Portugal) or representatives of employees (Austria), bar association and the police (the Czech Republic), banks (Finland), legal aid centres, legal aid insurance companies (both the Netherlands) and the office of ombudsman (Austria). However, it is worth mentioning that only very few of those specifically target data protection issues or are able to provide expert advice. On the basis of the fieldwork findings, the weak involvement of civil society organisations is linked to the lack of specialised ones (e.g. mentioned by interviewees from Poland) or the fact that none are available. In Greece, for example, none of the complainants interviewed received advice from an NGO or other civil society intermediaries.

Complainants in some countries also reported that they had received advice from informal sources, such as friends, relatives and others known to them (Bulgaria, France, Hungary, the Netherlands, Poland and Spain), either in person or by social networks.

"I was told by a lady, who is in my Facebook contact list."
(Complainant, Bulgaria)

The internet is another popular source of information about possible redress, especially during the initial stages of looking for information (including finding out about the data protection violation itself). Many complainants in most of the countries studied mentioned it. Nearly one in three complainants from the Netherlands said they found information on the internet, mostly on the websites of the NGOs. However, some of the interviewees (e.g. in Poland) maintained that there was no website that would offer a comprehensive guide to the available redress mechanisms or list stages of the proceedings, rights and obligations of individuals pursuing legal procedures. Others noted that the accessibility of the websites might be improved (as mentioned in Germany), or that, although the websites were described as very useful, they were too general or did not deal with the particular situation that the victims were faced with (e.g. in Romania). The importance of the internet as a source of information was demonstrated by fieldwork results in Hungary, which highlighted that websites were particularly helpful for people living in the countryside, as well as for those with less support from family and friends. Also, few respondents from Hungary mentioned online forums as important for sharing information and getting advice. Practising lawyers in Greece suggested that the DPA should have a more user-friendly website; furthermore, they proposed seminars and workshops to inform lawyers in general. Complainants from France mentioned the media as a source of information.

Despite the various ways in which people can get information, the importance of prior knowledge should not be underestimated. Most of the complainants interviewed maintained that they lacked information, and were not well informed about the data protection violations and redress available (as mentioned by complainants from the Czech Republic, Greece, Poland

and Romania). Also, one in three complainants in the Netherlands said they had to figure everything out by themselves. In several countries, complainants already had information about redress mechanisms and the laws supporting their case, owing to professional acumen or previous experience with redress procedures. Instances were noted in Austria, Bulgaria, Finland, France, Germany, Hungary, Latvia, the Netherlands and Portugal. The Finnish fieldwork found that, for several complainants, knowledge of the various redress mechanisms had been essential, as it made the process of finding out about and deciding which would be the most appropriate mechanism much easier. A Latvian complainant put it succinctly: *"The fact that I am a lawyer helped me a lot"*.

"Partly in my case it was really clear that it is due to my occupational background, I am constantly dealing with these issues. The other things are media reports that point out, for example, that the terms and conditions of different social media networks have been changing once again and so on, and then it is in the media. The third thing is of course my own use of social media, where I can draw my conclusions and inferences about data handling in the background, if you see for example what happens sometimes or what is recommended to you or something like that." (Non-complainant, Austria)

The opinions of the complainants and non-complainants on the lack of information received strong support from the intermediaries that support the victims of data protection violations, from the representatives of the national DPAs and from the legal professionals. Most people do not know where to find information on the laws governing data protection violations and appropriate remedies, and are not aware of the organisations and institutions offering legal advice and support. For example, several complainants interviewed in the Netherlands said that, although in theory information was available, in practice it was not easily accessible for people, as it was hard to find.

"It's so simple, the knowledge is so limited and people don't know that you can complain, where you can complain, how you do it, so that's the biggest problem." (Complainant, Austria)

"There is a lack of awareness of individuals about the fact that their rights have been violated. People often do not know that they can resolve their situation through the lens [originally 'prism'] of data protection." (Lawyer, Latvia)

"The heart of the matter is that people do not know what the right to data protection covers and what it does not cover." (Intermediary, Spain)

"The main barrier, as we were saying before, is the lack of an extended knowledge and culture about the mechanisms that could be used and also the fact that many times people renounce to specialised counselling from the very beginning, which may lead to them not choosing the most appropriate way to channel their complaints." (Lawyer, Spain)

The majority of the complainants in the 16 EU Member States covered by the research choose to seek redress through the national DPA. This is also the preferred option for those who considered seeking redress but, for whatever reason, chose not to pursue it. Complainants say they opted for the DPA over other alternatives for a number of reasons, including: lower costs; shorter duration of proceedings; less procedural complexity; the possibility for individuals, without legal representation, to initiate and use the procedure; advice received; the competence of the authorities; and the limited availability of other procedures.

Complainants in all 16 EU Member States surveyed were more reluctant to initiate court proceedings because of the greater costs, longer procedures and the perceived need to be represented or assisted by a lawyer. Criminal law measures do play a role in certain cases, but are used, with some notable exceptions, only rarely in the EU Member States covered by the research.

The choice of redress mechanism hinges on the information available, which is typically insufficient, and the advice received. Based on their awareness of the issues, those who have experienced data protection violations can be divided into two groups. The majority of the interviewees said they lacked information. The second group, a minority of 'well-informed' interviewees, said they had enough information because of their professional background, typically legal, or previous experience.

4 Assessment of the remedies

A separate set of interview questions addressed how to assess the different aspects of the remedies that the subjects of the data protection violations used. The data collected covered levels of awareness about their availability, the procedure, available support and satisfaction with the outcomes. The interviewees were asked to identify any obstacles when seeking redress, in particular the procedural aspects such as the length of the procedures, costs, legal advice received, burden of proof and any other issues faced. They were encouraged to share their opinions on possible improvements in the access and effectiveness of the remedy used.

The cases filed had different outcomes. Close to half of the complainants interviewed were successful after filing a data protection complaint. Regardless of the outcome, they expressed criticisms regarding the length of procedure or the fact that the decision had not been executed (at the time of the interview) or that the rectification requested was not sufficient to redress the violation. In one third of the cases, complainants were still awaiting a decision. Around one fifth of the complainants stated that their complaints were dismissed, that the procedures had not started or that no decision or action had been taken.

The opinions of the complainants tend to differ and depend on the outcome of the redress procedure. If there is a decision in favour of the complainants, the respondents tend to be satisfied with the remedies; conversely, they are not pleased with a negative outcome. However, in some countries (e.g. the Netherlands and Romania) the interviewees are generally satisfied with the procedures, but do see a need to improve the implementation of the decisions. In some countries (e.g. France and Greece), there is a general level of satisfaction with the DPA, but a negative evaluation of the judicial proceedings. Finally, in Bulgaria and the Czech Republic the majority of interviewees report dissatisfaction.

The other research target groups (representatives of the national DPAs, judges, practising lawyers and intermediaries) were asked to express their opinions about how accessible the redress procedures are for the subjects of the data protection violations; in particular, what legal advice and support is available and what barriers the subjects can face (especially in terms of information, deadlines, costs, documents to be provided and burden of proof). The professionals participating in the research were also asked to share their views about the level of expertise and specialisation of courts to deal with redress mechanisms in the area of data protection, about the measures that could contribute to dealing with the issues better and what could improve the accessibility and effectiveness of the redress mechanisms.

4.1. Obstacles related to the procedural aspects of the remedies

4.1.1. Length of proceedings

The interviewees were asked their opinions on the time spent when seeking remedy. As discussed earlier under the reasons for seeking remedies in cases of data protection violations, the prospect of lengthy and time-consuming procedures makes people turn away from seeking redress. The length of proceedings can be considered a significant barrier.

As might be expected, proceedings with a national DPA are significantly shorter on average than judicial proceedings. A number of EU Member States impose a time limit on proceedings for DPA redress mechanisms. For example, in Bulgaria, there is a statutory time limit of one month within which complaints have to be examined. In Italy, a decision must be provided within 60 days from the date of the complaint is filed, unless a further extension of 40 days is granted, which would then lead to a maximum duration of 100 days. In Poland, the Inspector General for the Protection of Personal Data (GIODO) must issue an administrative decision within 30 days, and, in Spain, the DPA and the ombudsman must issue a judgment six months from the time that the procedure has been initiated. In other Member States, proceedings are estimated to vary from Bulgaria and Poland's one-month time limit to instances reported in Germany where individual cases before the DPA can take over two years. Of the 16 Member States researched, 13 report that the majority of cases before the DPA are dealt with inside six months.

Respondents had varying perceptions of the length of proceedings before the DPA, although most respondents stated that they considered proceedings to be of an acceptable length. Respondents from Finland and the United Kingdom commented that proceedings were too lengthy. In Finland, some of the practising lawyers surveyed opined that the procedure was quite long despite being significantly shortened over recent years. In the United Kingdom, respondents in the intermediaries' focus group discussion and most of the complainants who were interviewed considered that the various remedies were too lengthy.

"After the complaint was lodged, there was a vacuum. I understand why but one can't do everything. [...] This is a failure on the part of the DPA, it doesn't give any feedback." (Complainant, Portugal)

"It took nearly one year. I made the complaint in June of 2010 and was answered in May 2011." (Complainant, Spain) [The complaint was lodged with the DPA.]

Respondents from both Bulgaria and Hungary felt that the DPAs were overly restricted by the deadlines imposed by national legislation. For example, the complainants from Bulgaria stated that they were satisfied by the time limits of the proceedings before the Commission, which were reasonable (around two to three months) and were respected. In Bulgaria, although the average response time was considered sufficient, the statutory one-month time limit for the Commission to examine complaints is considered by officials to be insufficient and often difficult to observe because of difficulties in the collection of evidence, communication with third persons by post and delays in their response. Thus, only in half of the cases are they able to respect this time limit. Similarly, in Hungary, interviewees from intermediary organisations think that the new two-month deadline is not enough to complete the entire procedure satisfactorily.

"Time is definitely a huge obstacle, because the process of collecting all the necessary documents and proofs is very slow and time-consuming. Usually, about 30 days would pass before I received a response from the DSI, as this is a time-frame for state institutions. Then communication between DSI and the Register takes 30 days again. [...]. And if we evaluate how much every hour costs – I could do something else". (Complainant, Latvia)

Despite these concerns, respondents from Italy, Romania and Germany noted that proceedings before the DPA have an acceptable average duration. Some members of the DPAs considered the complaint proceedings to be very fast and flexible. Members of the DPA in France pointed out that reducing the average length of procedure is a priority for the DPA, in spite of an expanding volume of complaints.

"The procedure usually lasts for at least about six months. It is a slow procedure but given the resources that the data protection agencies have this duration is understandable. But for citizens, who do not have as much information as us, six months is evidently too long a period and clearly discouraging. In our opinion, the procedure should be much faster." (Intermediary, Spain)

When redress is sought through the judicial system, proceedings can be much longer. Respondents from most EU Member States reporting average times of over one year. Often, they commented that the length of proceedings can vary greatly. By way of example, one judge in Austria estimated the average duration to be anything from two weeks to two years. At the lower end of the scale, respondents in Hungary estimate proceedings to take anything between six and ten months, whereas Latvia at the other end of the scale reports criminal cases lasting more than five years. What is clear from the responses is that the length of proceedings depends very much on the intricacies of the individual case, as well as the type of court. For example, interviewees from Hungary report differences in duration depending on whether the court in question is located in the capital city or the countryside. Budapest courts are overworked and thus subject to lengthier delays. Proceedings take longer at the United Kingdom's Supreme Court than lower courts.

"[In the case mentioned above,] 2007 is the year when the incident happened; the procedure has not been completed in 2012 and remains in the stage of an appeal. [...] [Other] cases are very different, with different duration. Problems during the pre-trial proceedings are due to the time taken before the presentation of allegations. The next problem is the ability of the first instance to review the case properly." (Judge, Latvia)

The assessments of the duration of judicial proceedings confirmed that the time taken is too long. Only respondents from Germany commented that the duration of the procedures was not considered a problem, whereas practising lawyers in Finland commented that the duration of court proceedings is considered reasonable only if they take less than two years. In Austria, the Czech Republic, France, the Netherlands, Poland, Portugal, Romania and the United Kingdom, lawyers, judges, complainants and non-complainants interviewed all thought proceedings too lengthy. Respondents in Portugal reckoned that some reasons for the long durations are difficulties in transnational cooperation, lack of resources and the complexity of some data protection violations. In Portugal, there is a specific mechanism exclusive to the administrative jurisdiction, called a subpoena for rights protection, liberties and freedoms. This allows a very quick decision (three days) by the judge and directly applies to the protection of personal data. Two of the interviewed judges in the Czech Republic noted that the duration of procedures is so long that the mechanism becomes ineffective. According to some judges interviewed, the Netherlands has relatively short procedures in administrative law and deadlines are properly observed. Moreover, several courts generally strive for prompt decisions, within a maximum of three months, even though there are no periods defined by law.

In looking at the responses collected, it is clear that the majority of those surveyed criticised the length of judicial proceedings, even when those respondents were practising lawyers or judges. Although criticism of the length of DPA proceedings was not as widespread, it is interesting to note that DPA staff refrained from directly criticising the length of DPA proceedings. DPA staff in Hungary noted that there are many differences between the different types of cases, which have an impact on the length of proceedings. DPA staff in Poland noted that, in some cases, the length of the proceedings conducted by the GIODO is affected by the need for interdepartmental consultations within the GIODO office. In Latvia, the DSI noted that the duration of proceedings depends to a large extent on its capacity, as well as the need to collect evidence. In Italy, representatives of the DPA consider the complaint proceedings to be very fast and flexible.

The time dimension mentioned by the complainants and intermediaries referred not only to the timely resolution or long duration of the procedures themselves, but to the time-consuming activity. The procedures were complicated, and difficult to understand and follow for those who lacked information about the process. As a complainant from Portugal put it *"There was nothing going on. There was never an actual, direct, concrete feedback"*.

Another issue related to time was the procedural deadlines. Perceptions contrasted across the target groups and the countries. The assessment of the deadlines ranges from considering them adequate and fair (examples provided by the respondents from Austria, France, Italy, Latvia, Poland, Portugal, Romania) to short and strict and constituting a barrier for seeking redress. Short and strict deadlines were mainly seen as demanding a significant amount of time to collect the evidence and lodge the complaint (as noted, for example, in Bulgaria, Hungary and Netherlands).

> The majority of those who had experienced data protection violations found that judicial proceedings took too long. In contrast, they found the shorter proceedings before the national DPA more or less acceptable in length.

4.1.2. Costs

The procedural costs were also discussed in the assessment of the procedures. The fieldwork results highlighted two key elements in the costs incurred by complainants and non-complainants: the cost of hiring a lawyer and the costs inherent in the procedure.

The cost of legal representation

Considering the importance of legal assistance in data protection cases, the availability of, and access to, cost-free legal assistance plays a key role in the decision to embark on a particular path. Legal aid and other ways of making redress mechanisms cost-free help more people to gain access to these mechanisms. However, limitations on legal aid restrict access to redress.

In most of the 16 EU Member States researched, costs and financial risk were among the major concerns individuals had when deciding to initiate or continue their case (Austria, the Czech Republic, Finland, France, Greece, Hungary, Italy, Latvia, the Netherlands, Poland, Portugal, Romania and Spain). In procedures where legal representation is mandatory, this is an important consideration for complainants, as hiring a lawyer can be expensive, particularly one specialised in this area of law. For example, a non-complainant from the Netherlands maintained during interview that she did not initiate a redress procedure because she lacked the financial means to pay for a lawyer. People made similar comments in Germany, Italy and Romania.

"Complainants are in favour of doing everything that it is possible to do (to lodge a criminal or a civil lawsuit, to ask for an indemnity, to address the Supreme Court) provided that there are no costs attached, but when there are costs they want to do nothing save addressing the Spanish Data Protection Agency, which is a free-of-cost procedure despite its limitations." (Lawyer, Spain)

Where legal representation is not mandated, complainants can reduce the costs considerably by representing themselves. However, self-representation may not be preferable, owing to the complexities of this area of law. Still, it does give complainants the opportunity to bring claims who might otherwise not have done so.

"So there are some costs, but if you don't have a lawyer, which I only had when I was obliged to by the law, when the case went to a higher-level court, plus my lawyer was really forthcoming and didn't charge that much. He understood that this was not about money. He was a fair man. So this didn't make me go broke. Plus when things take 10 years and the costs are a few thousand crowns, you can handle it." (Complainant, Czech Republic)

The procedural costs

As mentioned previously, the individuals subjected to violations tend to prefer remedies that do not involve costs. One reason is the difficulty in obtaining legal aid in cases of data protection violations. The high cost of judicial procedures often dissuaded complainants from approaching the courts, even if upon winning the case they could get compensation (examples provided by the respondents from Greece, Italy, Latvia and Romania).

High procedural costs in civil legal proceedings, including court fees, were also a problem for respondents in many EU Member States researched (e.g. Austria, France, Germany, Greece, Hungary, Italy, the Netherlands, Poland, Portugal, Spain and the United Kingdom). For instance, the judges interviewed in the Netherlands estimated the costs of a civil procedure (in which legal representation is required by law) at between €500 and €100,000, with court fees of €150–€200 for individuals and €300–€500 for collective complaints. In addition, the losing party in a civil procedure will be ordered to pay all costs incurred by the defendant, which can amount to thousands of euros. According to the judges interviewed, plaintiffs will not be fully reimbursed for the money they spent on legal representation if they win the case, because market prices are higher than the reimbursement prices established by law.

"In civil procedures you have got a lawyer, but not many lawyers are familiar with this Act. But if you need a lawyer, civil proceedings are just too expensive. [...] Civil procedures easily cost a few thousand euros and that is a lot." (Judge, Netherlands)

"Compensation will certainly not cover the expenses. Compensation covers neither material loss nor moral harm." (Intermediary, Latvia)

The interviewees assessed the costs as a central barrier to obtaining legal protection in cases of data protection violations, as the costs were often high and unforeseeable. It was common for costs to exceed awards. High costs were the main reason many affected persons did not pursue the case further (evidence from respondents in Austria, Finland, Germany, Greece, Hungary, Italy, the Netherlands, Poland, Portugal, Spain and the United Kingdom). Also, the lengthy proceedings tended to increase lawyers' fees and court costs.

"I did hesitate for a while, because I know it would cost me €150 to appeal. That €150 was really the limit. Finally I decided it's worth my principles. Even in case of a rejection. But not much more. For €200 I would have chosen not to do it." (Complainant, Netherlands)

"Court case costs are very high in Portugal. The price is the system's inefficiency because court cases take a long time and lawyers' fees are interrelated with this, because the systems' inefficiency implies more hours of the lawyer's time. These questions are extremely relevant. The court costs themselves are low." (Lawyer, Portugal)

"I would say the biggest obstacle is costs. And costs associated to a relatively distant and uncertain outcome, and uncertainty is another problem of our justice system in general." (Judge, Portugal)

"You need someone who is really knowledgeable, an expert. And then there will be costs; why should you consider paying them if the outcome is so uncertain?" (Intermediary, Germany)

"I mean, it's not about whether or not you get it back or not if you win, but you need to pre-finance it for a longer period of time, a few thousand euros of pre-financing." (Lawyer, Austria)

"As I was successful all costs were reimbursed. But you certainly have always a cost risk. This means that you have to be prepared to bear the costs by yourself. And this will become a bit more expensive at the moment when an appeal is lodged and the opposite side hires a law firm. If I had to pay this, this would have been significant. Well, I believe that many people can't afford to pay a four-digit sum, nor they are prepared to do so from their own resources when they lose the case." (Complainant, Germany)

"I mean, if the result is that of obtaining a symbolic compensation, and to go on for years paying a lawyer, I haven't the faintest idea, €15,000–€10,000, to obtain €800 of compensation and maybe go to court eight times, because unfortunately you go to testify many times, you return again, etc., in terms of the costs and benefits, this type of action is not facilitated in Italy. It should be something simpler and more within reach, much more in keeping with incomes, needs as well as the necessity to balance this with other interests." (Judge, Italy)

In some of the EU Members states researched, the procedural costs are relatively low (e.g. Bulgaria, the Czech Republic or Romania) and the legal representatives or intermediaries interviewed described them as not a great problem and not creating specific obstacles or any significant financial burden for the complainants.

"As far as the costs are considered, I think that the court services are provided virtually for free. There is no such country where one can run through the whole system for BGN 15 (€8). […] More than affordable." (Judge, Bulgaria)

"Procedures regarding data of public interest are free of charge, but other costs depend on other factors such as (1) the cost of the legal representative; (2) the outcome of the procedure; (3) the amount of compensation wanted. The value of the sum of the dispute set by the courts is now HUF 36,000 (€125) at least. An average case costs at most HUF 50,000 (€174). According to the relevant act, currently the duty cost is HUF 15,000 (€52), which is not big enough to be a deterrent factor for complainants. These types of procedures are not among the 'expensive' ones." (Judge, Hungary)

However, the legal representatives from the countries with comparatively low court fees and a lower financial threshold maintained that this encouraged the citizens to file unmeritorious claims. Also, the judges interviewed maintained that low costs meant that many cases were transferred to the courts, whereas efforts should be made instead to solve them outside the courtroom. For instance, in Latvia, whereas several research participants considered the state fee in the administrative proceedings quite high, the judge said that, because courts had such a heavy case-load, the fee needed to be raised depending on the amount of compensation requested, with a view to preventing unfounded applications.

"I believe that the state fee is favourable to the complainants. We even think that the fee should be a percentage of the requested sum, similarly to Estonia, in order to prevent unfounded applications – our case-load, therefore, is so big." (Judge, Latvia)

"Costs should be calibrated. They should be affordable and not prohibitive but not too low, otherwise justice is not done." (Judge, Greece)

Respondents considered costs, whether procedural or for legal representation, an important barrier to accessing remedies in the field of data protection. Lengthy procedures with uncertain outcomes tend to raise costs, which might also mean that costs outweigh any potential benefits.

FRA opinion

Victims of data protection violations are dissuaded from pursuing cases for several reasons, including costs and difficulties associated with proving data protection violations.

EU Member States should consider promoting support through legal advice centres or pro bono work. These support mechanisms should be complementary to, and not a substitute for, an adequately resourced legal aid system.

4.1.3. Legal representation

Research participants were asked to assess legal representation in terms of its availability and quality. Not all redress mechanisms in the data protection area require legal representation. The remedies which do not require legal representation are often preferred (e.g. hearings before national DPAs), as they involve fewer costs for complainants. Nonetheless, according to the information collected, having a lawyer for assistance and representation is helpful because data protection law is complex and also because it is relatively novel, with little in the way of judicial precedents and practice.

On the availability of legal representation, responses were mixed in terms of the sources of the legal assistance and the costs of obtaining it.[55] There was both negative and positive feedback. Although there was widespread dissatisfaction with access to legal representation, a number of respondents from different EU Member States gave positive feedback. Interviewees from Bulgaria were the only ones to note that they did not need a lawyer for some of the proceedings before the DPA. In cases that required a lawyer, assistance was provided by DPA officials, lawyers and lawyers working in NGOs. More than half of Bulgarian respondents received legal assistance, which they considered of great help. Respondents in Hungary also noted that the courts provided free legal advice, as did NGOs and DPA officials. The judges interviewed in Italy pointed out that the availability of lawyers was not a problem. The research included five complainants from the Netherlands who were offered legal assistance by a privacy expert, legal aid centre or NGO. In Poland, among the respondents who sought remedies for personal data protection violations, only one hired and paid for a lawyer. Others received pro bono legal assistance.

Despite these favourable responses, interviewees in half of the EU Member States surveyed criticised the lack of legal representation available from both intermediaries and the judicial system. The interviewees from Austria reported that most intermediary organisations did not provide legal representation for clients. That opinion was echoed in Poland, where – despite pro bono assistance being available in judicial proceedings – it was stated that there was no intermediary organisation or association that provided free legal advice in the area of data protection. Again, interviewees in Portugal described the lack of associations and civil society organisations that could represent people's interests and rights in the field of data protection, while interviewees in Spain also bemoaned the lack of NGOs and associations working in the area. For example, only one

55 See similarly FRA (2011a).

NGO in Spain was identified as dealing with the defence of data protection rights.

In the United Kingdom, it was reported that, although there was provision for pro bono representation by lawyers in courts, such representation is the exception. The responses indicate barriers to access to legal representation. The United Kingdom interviewees complained that access to pro bono services was limited by the number of lawyers who were willing to take data protection cases without payment. The suggestion that lack of funding was the primary impediment to legal representation found support from representatives in both France and Finland. In France, the requirement for legal representation and costs associated with it kept complainants from bringing cases before the Council of State and Court of Cassation. Interviewees in Finland reported that there was a great demand for legal advice and support, but the costs prevented people from seeking it. On the other hand, even if the individuals are entitled to the legal assistance provided by the State, they might not be able to use it because no lawyer is available. For example, the practising lawyers interviewed in Bulgaria pointed out that legal assistance provided by the state was not applied in practice, as the system did not function efficiently. A similar situation was reported by the interviewees from Romania. In general, legal aid is reported as expensive and not easily available.

"Although persons in my situation have the right to free legal aid, in Romania this is not applied in practice."
(Non-complainant, Romania)

Interviewees in Latvia pointed out that access to legal assistance was quite limited, and there were not enough qualified lawyers and defence counsels. This chimes with the difficulty in finding judges and lawyers to interview for the fieldwork. In eight out of the 16 EU Member States covered by the research, there were too few judges in the field for the minimum number of interviewees to be achievable (Austria, the Czech Republic, France, Germany, Greece, Latvia, Romania and Spain). Likewise, it was hard to interview the minimum number of lawyers in the following nine countries: Bulgaria, Germany, Greece, Hungary, Latvia, the Netherlands, Portugal, Romania and the United Kingdom. Although the numbers of the interviewees were reached, some of the respondents of these target groups lacked sufficient experience and expertise (predefined in the selection criteria). This finding indicates that court cases in the area of data protection are rare.

In the search for potential interviewees, another issue surfaced that limits individuals' access to lawyers who have relevant knowledge and expertise: they tend to work as legal representatives of the private companies (the data controllers) more often than as representatives of the individuals. Respondents in Hungary, the Netherlands, Portugal gave examples confirming that the lawyers with proper expertise tend to represent private companies (being employed by the companies) and not individuals. Likewise, during the fieldwork in the Netherlands and Portugal, it was difficult to find lawyers who have assisted individuals seeking redress for a violation of the data protection rights, as most of them tend to work for the data controllers. To a certain extent, this problem is linked to the extremely low number of individuals using the courts for remedies in the data protection area and, thus, requesting the services of a lawyer.

It is mainly the complicated procedures of data protection law that cause the need for legal representation or would make it helpful. The subjects of the data protection violations expressed this view and the legal professionals strongly supported it – both judges and practising lawyers across the EU Member States researched.

"Although I had rather a good level of knowledge compared with an average person, [I needed a lawyer]. The dead end is connected with nuances – one can know that there is a breach, but he or she might not know what to do about it."
(Complainant, Latvia)

"Well, in theory the complainant can always file a complaint on their own, but I wouldn't recommend it to anyone. I would recommend it just as much as I would recommend someone to operate on their own brain." (Lawyer, Finland)

"But considering this a relatively marginal issue, a qualified attorney would be appropriate." (Judge, Czech Republic)

"There are an enormous number of requirements from a legal point of view. A law suit based on the institution of civil liability is extremely complicated in Portugal."
(Judge, Portugal)

"Yes, I think that because it is a complex activity, it is important to be assisted by a person with legal knowledge, able to assess the impact of such laws on the person's circumstances." (Judge, Romania)

Availability and access to free legal support is not enough: the lawyers that represent legal aid recipients should be knowledgeable and experienced in the area of data protection law. On the quality of legal representation, the findings of the fieldwork were much more damning. Respondents from 12 of the 16 EU Member States criticised the quality of the representatives available.

Whereas some of the respondents actively criticised the quality of the work of their legal representatives, the majority detailed how it was difficult to find specialised lawyers in the area of data protection. Accordingly, individuals had to make do with lawyers, who were less able to offer expert advice. Respondents in Austria, Bulgaria, the Czech Republic, Germany, Greece, Hungary, Italy, Latvia, the Netherlands, Poland, Portugal,

Romania, Spain and the United Kingdom all noted that there were only a few lawyers who were specialised in data protection. Therefore, the lawyers who were available lacked the expertise to guide and support complainants in the best way. In the Czech Republic, one of the respondents from an NGO pointed to the fluctuating quality of service provided by attorneys.

In Greece, lawyers were described as unfamiliar with data protection laws, although some complainants said that specialised lawyers worked for them. In Italy, lawyers are allocated by a computer that randomly selects a lawyer from a list, without considering whether he or she has any knowledge or expertise. This results in complainants being represented by lawyers who are not perceived as well-versed in the intricacies of this area of law.

"There are very few practitioners at the bar who specialise in data protection." (Lawyer, United Kingdom)

"There are no highly-trained professionals. There are no lawyers specialising in it since it is a quite new discipline." (Intermediary, Spain)

"There is no specialisation. We, in the general administrative chamber, work with 250 legal acts! Please, believe me, we try to do everything with the utmost degree of care, but you can't be the expert in everything. That's why I think it's not about some narrowly defined specialisation in this field. But we, at this point, considering the Personal Data Protection Act, Access to Public Information Act, this is the area which should be [treated as] some kind of specialist field, because, first, you would have a totally different approach if you hear a particular number of such cases." (Judge, Poland)

The criticism of the quality of the legal representation was aimed at both intermediaries and the judicial system. In Poland, staff members of the GIODO regarded the quality of legal representation as quite low. In Romania, lawyers described the redress procedure as complicated (as well as difficult for the complainants to follow steps in the procedure), requiring special knowledge of the legislation and technologies (e.g. social media). In Portugal, both lawyers and judges highlighted the poor quality of the legal aid provided by the state and indicated that it was inadequate because it served only a limited number of people, those whose level of resources was well below the acceptable minimum. Thus, an average citizen cannot gain access to legal aid. One of the non-complainants in Italy stated that the lawyer's lack of knowledge dissuaded him from pursuing his case.

"I honestly do not know if the lawyers (nominated by the State) are well aware of data protection issues." (Judge, Portugal)

"I don't think there is, on the part of the Bar, of lawyers, a professional specificity, therefore, there is no specific assistance. I think people make use of lawyers who deal with civil law." (Judge, Italy)

Some states are making promising efforts made to provide legal representation, but there is a shortage of financial resources for this. The concomitant lack of expertise in the field of data protection has serious consequences for the quality of the representation provided.

"Few lawyers specialise in this field, and if a person wants to obtain a favourable decision in their case, they simply cannot afford it." (Intermediary, Poland)

While discussing the specialisation of the lawyers, interviewees raised the need for professional training. The representatives of the legal professions and the intermediaries in many of the EU Member States especially mentioned it. The need is for both training during higher education and in-service training (or specialisation) during the course of a career. According to the respondents, gaps in expertise affect the ability of lawyers to argue complicated cases well. To manage such cases, they need specific knowledge.

"There is a whole issue of training and information for lawyers and not just business lawyers who will defend businesses. This should also concern lawyers in employment law, for example. These rules are not at all integrated into the training of lawyers. There are occasional lectures but that is not enough. It's the same for judges and trades unions." (Lawyer, France)

"I have seen a nearly absolute lack of training regarding both data protection and intellectual property in the Faculty of Law itself where I studied. In the five years I was there, I can say that I practically heard nothing about the Organic Law of Data Protection or about the right to data protection or about any specific rights on internet." (Lawyer, Spain)

"There is no extra training in that field; usually those judges preside over these cases, who would otherwise hear lawsuits in personality rights. There are meetings, conferences, where judges meet. [...] Given that the legal field is rather big, anyone who deals with such lawsuits has once been a beginner, otherwise you cannot start it. Then the judicial practice ... and it can be learnt from the anonymous resolutions and different databases. I think that the colleagues, [judges] have enough experience in that, although judges do not confront this area to the same extent. I don't think that there is any judge who would specialise in that." (Judge, Hungary)

"The fact that there are hardly any lawyers is related to the fact that the lawyers ultimately don't earn any money from it. So, in that sense one can only say – the opportunity is to welcome, it's in any case to recommend them to other offices that are officially qualified to deal with such matters, otherwise the chances of success are very low and rare." (Intermediary, Austria)

The Italian DPA staff members mentioned the training sessions organised by the DPA for interested parties from both public and private sectors, during which practical cases were analysed. In Hungary, several data

protection training programmes are offered and organised by universities (mainly courses on data protection or related topics) or private firms (mainly one-day training). Since 2012, the Hungarian DPA has organised a series of conferences of internal data protection officers.[56] Furthermore, in 2012, the Judge Academy and the Hungarian DPA signed an agreement to build data protection and freedom of information into the curriculum of the training.

The French DPA has established partnerships with the National School of Magistrates and the National Bar Council, offering training to lawyers and judges to bridge gaps observed in knowledge among legal professionals. Similar agreements exist in other countries, such as Hungary. Feedback is seen as positive and the training offers an opportunity for trained judges in the legal institutions to share experience. The DPA has also developed in-house training for judges and internships as a means of pre-recruitment. Beyond the DPA, interviewees also mentioned the development of academic and professional training in the field, with, for instance, specialised Masters programmes and continuous training developed for engineers by a specialised school, covering data management or technical and legal compliance challenges.

The lawyers interviewed during the fieldwork also drew attention to the need for technological, digital expertise in relation to the area of data protection law. As already mentioned, participants identified internet-based activities as constituting the most frequent data protection violations. Relevant expertise is needed to manage cases that involve, for example, illegal data processing in databases, websites or any other digital technologies and instruments. The respondents from Bulgaria, Italy, Portugal, Romania and Spain shared these opinions.

"We need more training on new technologies, on the use of the internet, on terminology, because there are things we don't understand and some claims regarding very advanced technology are very complicated. Google is a typical case in which we find that the parties know much more than we do. And the lawyers as well, because they have technical experts advising them, as they work for large companies with plenty of means." (Judge, Spain)

The fieldwork carried out in the 16 EU Member States indicates the perceived lack of a sufficient number of specialised lawyers in the data protection area. The respondents maintained, however, that this area is relatively new and is not as attractive as other areas of law because of the lower financial gains (e.g. opinions expressed by respondents from Austria, the Netherlands and the United Kingdom).

56 See National Authority for Data Protection and Freedom of Information (2013), p. 26.

The lack of accessible, expert legal representation and advice, the lengthy and time-consuming procedures and the costs involved can dissuade those who have experienced data protection violations from pursuing their cases. Complex processes, lack of awareness and non-specialised support also demotivate individuals and kept them from seeking redress for data protection violations.[57]

FRA opinion

Legal professionals rarely deal with data protection cases, so they are not aware of the applicable legal procedures and safeguards. There is a lack of judges specialised in this area.

The EU could financially support training activities for judges and lawyers on data protection legislation and its implementation at Member State level. EU Member States should seek to strengthen the professional competence of judges and lawyers in the area of data protection, providing training programmes and placing added emphasis on data protection issues in the legal curriculum. This would increase the availability of sufficiently qualified legal representation.

Strengthening professional competence would also help reduce the length of proceedings. The gap in such competence is one of the barriers to seeking redress before courts, as confirmed by the 2011 FRA report on Access to justice in Europe: an overview of challenges and opportunities *and by the findings of this fieldwork.*

4.1.4. Burden of proof

As far as the burden of proof is concerned, the situation clearly varies, depending on the EU Member State covered and the procedure used for seeking remedy.

Most of the complainants interviewed during the social fieldwork mentioned difficulties they encountered in providing sufficient and complete evidence. The complainants interviewed in the Czech Republic, Greece, Latvia, Portugal, Romania and Spain clearly indicated the burden of proof as a barrier to seeking remedies in the area of data protection. The problems are associated mostly with difficulties in proving the data protection violation, mainly regarding internet-based activities, and several practical obstacles related to obtaining evidence in the specific field of data protection. This was also the opinion of the lawyers and intermediaries interviewed, whereas some judges considered the burden of proof to be acceptable (e.g. Portugal, Romania).

57 See also FRA (2012c).

"The hardest thing is to document. You have to show solid evidence, even material evidence such as papers, documents, things that convince the judge that you suffered damage." (Intermediary, Romania)

"Burden of proof is quite a big problem in Latvia. A person has to prove his/her case by him/herself. And even then there is no guarantee because the data have always been forged, especially in medicine. Even the best advocates, for the most part, are not medical doctors. And our judges are not specialists in the health care field." (Intermediary, Latvia)

"As I see it, it can be a very political question. So it's something that I do not see as a judicial issue. And there, in my opinion, should never be an inversion of the burden of the proof in these cases, that is, the accused may never be obliged to prove he didn't commit those violations. [...] This would bring distortions in society, distortions that would really be irreparable." (Judge, Portugal)

"I don't think it is hard to prove. I don't think the burden of proof is reversed or at least in the first phase it is not reversed. So the burden of proof stays with the complainant that alleges the right violation. How? You come and bring evidence – a printout from the internet, a request and a reply from the authority brought to justice or, I don't know, if needed a witness who was with you when the authority communicated their reply ... Afterwards there might be some variations, like in the case we talked about, the defendant alleged that the information remained on the internet for a very short time. Then the burden of proof turned to them to show for how long the information was online." (Judge, Romania)

While analysing the research data from the EU Member States covered by the research, different patterns can be identified. In some countries, all of the target groups interviewed share a unanimous opinion, whereas in others it differs according to their procedures and experiences. For example, respondents from Bulgaria, Italy and Poland did not consider the burden of proof to be a problem. In Bulgaria, the rules addressing the burden of proof were viewed as relatively simple and adequate. In Italy, in DPA proceedings, the burden of proof is reversed, putting a duty on the data controller to prove that data has been lawfully processed. Interviewees in Italy unanimously pointed out that the burden of proof always lies on the plaintiff in the Italian judicial system. In Poland, the civil law creates a number of presumptions that operate in favour of the claimant.

"Here, the injured party is in a much better position than in typical proceedings. They only have to show that their personal interests have been infringed upon, through a verbal or written statement or in any other way. So a person has to attach evidentiary documents or other exhibits confirming the circumstances of the infringement, and that's all. [...] There is a presumption of unlawfulness of the respondent's action. And this is the respondent who has to prove that he or she had consent to disclose personal data. [...] The injured party is much better positioned in proceedings for the protection of personal interest." (Judge, Poland)

Other examples provide differing opinions with regard to the burden of proof. In Austria, intermediaries, lawyers and some complainants interviewed found it difficult to provide evidence, whereas the judges and some other complainants did not perceive the burden of proof as troublesome. In France, most of the complainants did not encounter specific obstacles in providing the national DPA with evidence. The lawyers and intermediaries interviewed, however, pointed out that the burden of proof could be a problem. In Germany, the opinions clearly depended on the procedure used: none of the interviewed groups mentioned the burden of proof as a specific problem when lodging a complaint with administrative or social courts, since the judges at these courts follow the principle of ex officio investigation. The burden of proof was, however, seen as a key issue when taking data protection cases to the civil courts. In Finland, the majority of the complainants who faced the burden of proof considered it easy, whereas the practising lawyers thought that it was rather difficult for complainants in cases of data protection violation in the health care field. In Hungary, in most cases the burden of proof is reversed and the petitioner is in a favourable situation. Problems arise when the evidence is not concrete, as providing proof is difficult in these cases. In the Netherlands, several complainants and judges interviewed did not think it was difficult to prove the violation of data protection. However, most intermediaries and lawyers interviewed held a less favourable view. In the United Kingdom, the judges and the representatives of the national DPA took the view that the burden of proof did not constitute a problem, whereas the intermediaries and lawyers considered that satisfying the burden of proof could be difficult for complainants in some cases. Most complainants reported difficulties providing evidence, especially when the violation involved access to data.

"Q: OK, and what about other required documents or for example the burden of proof?"

"A: It doesn't play that much of a role in constitutional procedures, because the fundamental right to data protection is legally reserved and hence the Constitutional Court only conducts a rough check. Simple legal guidelines, on the other hand, are rather treated by the Supreme Administrative Court, so the Constitutional Court does not conduct any complicated investigations. So in our case, the complainant does not need to provide any additional evidence, it doesn't play a role for us." (Judge, Austria)

In contrast to other issues discussed, respondents' views on the burden of proof vary considerably, reflecting country and target group differences. Complainants, intermediaries and the practising lawyers interviewed tend, more frequently than the judges interviewed, to define the burden of proof as a problem. They speak of issues in providing sufficient and complete evidence, especially regarding internet-based activities.[58]

FRA opinion

Rules on the burden of proof should be streamlined, especially in cases concerning internet-based activities.

4.2. Obstacles related to the role of the national data protection authorities in effectively remedying data protection violations

The DPAs play a crucial role in remedying data protection violations, and FRA data showed their ability to take a range of actions, including issuing administrative sanctions. However, the qualitative social fieldwork on remedies in the data protection area carried out in the 16 EU Member States identified several critical issues related to the activities of the national DPAs. Opinions were voiced by the representatives of the national DPAs themselves and by other target groups interviewed.

Participants in various EU Member States expressed criticism of the national DPAs. In some countries they questioned the independence of the authority or described it as not completely independent (as noted in Austria, Bulgaria, the Czech Republic, Hungary, Italy, Latvia, the Netherlands, Spain and the United Kingdom). Among those citing limited independence, interviewees mentioned appointments of the DPAs' governing staff members by political bodies, supervision by certain institutions (e.g. specific ministries) and limited action taken against other public institutions in cases of data protection violations.

During the focus group discussions, representatives of the national DPAs highlighted the limited human and financial resources necessary to ensure that they run efficiently and effectively as independent supervisory authorities. According to the interviewees, the resources at the disposal of the DPAs should include sufficient numbers of well-trained, qualified staff with legal and technical expertise, including specialised knowledge, as well as strong technical departments with access to the latest technologies. This was regarded as essential because violations were often linked to the use of the internet and other technologies. The interviewees related the lack of technical expertise to the perceived inability to gather evidence. Professional, expert staff would significantly improve the investigatory abilities of the authorities. The representatives of the national DPAs said they needed not just to have sufficient staff, but also to have the right mix of competences amongst the staff (e.g. lawyers, computer scientists and technology experts), as well as investment in proper training.

Representatives of DPAs in several EU Member States covered by the research said that the national DPAs were underfunded and understaffed. Their budgets did not allow for high-quality specialists to be hired and new, cutting-edge technology to be acquired for the collection and analysis of evidence. This viewpoint is supported by the findings of FRA's paper on the independence of DPAs.[59]

"More staff [is needed]. If we had more people, we would be able to process more. Now it is sometimes frustrating that we cannot process certain things just because we do not have the capacity. That is quite an obstacle." (DPA staff, Netherlands)

"The issue of material and human resources remains absolutely essential." (DPA staff, Spain)

"An authority like ours, while having legal experts as a core group, has an increasing need for more computer science and technology experts. So, to me, that is what is a bit lacking. We surely need more staff specialised in this area. To improve our effectiveness, this could certainly be a point as well as training, both internal and external." (DPA staff, Italy)

The lack of financial and human resources has a negative impact on the quality and quantity of the DPAs' work, and limits their ability to control and sanction data protection violations. For example, the complainants interviewed in the Czech Republic and Portugal said that the lack of financial and human resources resulted in the cases not being accepted or no response from the authority being received. Some of the representatives of the DPAs stated that the amount of work that the DPA currently had was at the upper limit, and they could not handle more with the resources available (e.g. DPA staff from Finland, Poland, Portugal and the United Kingdom). The issues discussed above affect the way the national DPAs are perceived by the public.

"What they said in the email they sent me was that they had a large number of complaints to deal with and few resources to handle them." (Complainant, Portugal)

58 See also FRA (2012c).

59 FRA (2014 forthcoming).

There are examples of DPAs minimising the impact of understaffing, and they report good practices designed to assist victims of data protection violations. In France, for instance, the DPA is understaffed but still provides support to clients: general information, orientation and counselling before the formal complaint procedures, and also advice on ways to exercise the right of access directly. The hotline, which gives access to legal professionals as well, handles a lot of the requests for information before a complaint, and resources are available on the DPA website too. Information is also disseminated among clients through online fact-sheets and thematic guides addressing core areas of concern, as well as a general radio programme developed in partnership with a news radio station (France Info), with thematic angles and concrete examples based on actual cases reviewed by the DPA. Specific DPA initiatives included the online complaint facility developed in 2010. According to the DPA's figures, that is increasingly used by individual complainants and has already proved its worth. Interviewees also mentioned an online template generator that provides model letters to request access or modification or deletion of personal data. The resource mentions relevant legal standards and obligations. Not all complainants may not be aware that such a service exists.

The representatives of the national DPAs themselves were critical of their public relations and communication with the complainants. When asked about the feedback received from their clients, representatives from different EU Member States said that, in general, there was little feedback and it very much depended on the decision taken. According to the DPAs, complainants usually give negative feedback when the answer received from the authority differs from what they had expected or hoped (e.g. in Austria, Finland, Germany, Italy, the Netherlands, Poland and the United Kingdom). The interviewees mentioned that the negative feedback was also related to the duration of the procedure, timings, the clients' desire to know when they would get a response, and their lack of understanding of the content and limits of the procedure. The DPA representatives said that dissatisfaction was related to not knowing what had happened to the complaint and whether anything was even done about it.

"Sometimes people complain about the ombudsman procedure, and that's the case when people just don't know what the goal and aim of an ombudsman procedure actually are and where our limits are. We then certainly explain, and say 'we can't just go there, for example, and cut through the wire of the video camera'. Yes, so sometimes there is just a wrong understanding of the procedure and that one actually needs to go to court." (DPA staff, Austria)

"What is mainly criticised is not that we are lacking independence but that data protection does not work. When complainants are not successful in seeking redress they say: 'forget data protection.' This is the image of a toothless tiger, a paper tiger. [...] For this reason the power of issuing orders was important for us; because what counts is to achieve and enforce things and not only to issue penalty fines." (DPA staff, Germany)

"Often we do not even say whether an investigation is in process, or what we have done with it. The reason for that is, if we do that, the complainant knows whom it concerns. Both sides have not yet been heard then." (DPA staff, Hungary)

"When people are complaining to us, they are complaining because they believe they're right, they are not coming to us for an assessment, we are coming from neutral territory, they're not, they absolutely believe they are right, otherwise they wouldn't be complaining. So if you don't find in their favour it's inevitable that they are going to be annoyed with you and they are going to think that the ICO is doing something they shouldn't be, when in actual fact that is not the case at all." (DPA staff, United Kingdom)

The research participants considered it important that DPAs raise data controllers' awareness about the legislation and its application. As an example of sharing their expertise, the DPA staff and the lawyers from the United Kingdom said that the authority did an immense amount of highly valuable work in educating the public about data protection law.

"[ICO is] an approachable organisation from which data controllers can seek advice as to procedures they need to follow to ensure compliance without fear of the imposition of sanctions." (Lawyer, United Kingdom)

Representatives of the other national DPAs shared their experiences in awareness-raising. For example, the new Hungarian Privacy Act[60] prescribes a yearly conference for internal data protection officers organised by the DPA in order to maintain closer relations with experts and to have a common interpretation of the legislation. It also holds presentations on data protection, when needed, to inform people and explain data protection principles. The Polish DPA is involved in many educational activities, including organising conferences and seminars for scholars, educational campaigns, training courses, guides published on the DPA's website and other publications, which help make citizens aware of data protection issues. The Portuguese DPA makes all its decisions available online to all citizens and considers it an important awareness-raising tool for the general public.

While asked about the problems related to the implementation of the decisions, some of the

60 Hungary, Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Privacy Act).

representatives of the national DPAs did not mention any specific issues. The others shared their practical experience in highlighting areas for concern. The main problem mentioned was the inability to ensure that the instructions issued were implemented and fully complied with by the data controllers. Where instructions to delete data had been made, some participants mentioned that the workers' representatives were contacted to check if the decision had been complied with. Interviewees also noted that it was difficult to ensure that the public administrations did not ignore decisions and that they complied with any instructions given (as mentioned in different contexts by the representatives from Bulgaria, Germany, Greece, France, Latvia and Portugal). For example, according to the statistics of the Bulgarian DPA, one third of the sanctions imposed in response to complaints are complied with voluntarily. This proportion is smaller in the cases in which the sanction is imposed as a result of planned or ad hoc checks by the DPA. The examples revealed instances in which the data controller postponed compliance with the decisions.

"It is different, if you require someone to delete a database, they may do it in a ritual manner and bring you all kinds of evidence, but you can never be sure if they didn't make a copy, which they store illegally, or keep somewhere, for example, on another data storage devise. This is a problem, of course, everywhere, not only in Bulgaria." (DPA staff, Bulgaria)

In addition, the findings from the fieldwork suggest that private sector data controllers challenge administrative acts of DPAs in courts (examples mentioned in Germany).

The other area of concern was that the public administration – acting as the data controller – tended to ignore the decisions of the national DPAs, especially if the complainant did not take the case to court. Respondents also mentioned that the imposition of fines has only symbolic meaning, as it is the state that fines the state. In some of the cases mentioned (e.g. one from Greece), the authority cannot even monitor if a fine has been paid and it is not clear that the DPA's decisions are enforceable. It is up to those that violate data protection to comply. Respondents from France and Spain raised issues related to the transnational nature of internet services, and cases when the data controller was based outside the EU. Also, problems related to the investigation of cases can be mentioned in this context, as sometimes the data controller is difficult to reach.

"In the public sector, when we act as authority vis-à-vis another authority, we cannot issue orders or instructions." (DPA staff, Germany)

"No penalty fines, nothing." (DPA staff, Germany)

"In the public sector the problem is that the penalty has no meaning apart from having a symbolic character and it is not easy for the public sector to comply." (DPA staff, Greece)

Another issue related to enforceability is that an individual complaint may bring to light structural or systematic data protection problems. In order to solve the problems, several actors, even in different countries, might be involved and it can take a long time to achieve legal data processing.

"What the complainants report, well, for the area of police and justice are more or less individual problems behind which the structural problems are hidden sometimes. These need more time then. The individual complaint is quickly dealt with. Then we need to solve the structural issues with the authorities [discussants laugh]. *This can take one or two years sometimes."* (DPA staff, Germany)

"DPA's decision does not reach all branches of the [public institutions]. Because the public administration refrains from circulating the decision, thus the same cases keep coming from other branches. Here we urge them to publish a decision, to update their internal regulations." (DPA staff, Greece)

Some of the intermediaries expressed a negative opinion of the national DPAs (noted in Austria, Bulgaria, Greece, France, Italy and the Netherlands). The main criticisms were related to the DPA's communication and publicity; the effectiveness of its work; the perception that the authority was undertaking too many different roles; that it was understaffed; and that it was a 'watchdog without teeth'.

The DPAs' activities were compared with other national institutions (e.g. national ombudsmen). Some of the respondents cited a preference for the use of other institutions rather than DPAs. Others criticised all institutions responsible for data protection; they pointed out that all authorities' independence is limited if appointment criteria make them dependent on political power. According to the intermediaries, the national DPAs should become more independent and receive more powers, and the procedures should be more transparent.

"Here, the state is presented as the main violator that chooses an easy solution, i.e. to have an independent authority that cannot implement its decisions." (Intermediary, Greece)

Criticism targeted the publicity and transparency of activities, saying that the general public does not know the national authorities well enough ('not seen in the media', as indicated by the respondents from Bulgaria and Finland, for example). The interviewees suggested how to improve access for the complainants, making the procedures easier to understand. There is a need for more publicity about successful cases or timely and effective reactions to particular problems, which would increase awareness of rights and encourage people to lodge a complaint. One intermediary from Bulgaria suggested posting a sample complaint on the

authority's website to assist the complainants. Others from France thought that it would be helpful to develop guides concerning data protection and social network issues or that companies collecting personal data should point out the existence and the competence of the French DPA.

Also, the intermediaries tended to recommend that the authorities be 'more supportive' before and during a redress procedure. Those who maintained that the national DPA offers an efficient and powerful remedy also stated that it should improve the quality of its responses and carry out more communication campaigns.

Some of the intermediaries' main criticisms of national data protection authorities focus on poor communication, and insufficient transparency and contribution to public awareness raising. Some also question the independence of the authorities, mainly because of possible political appointments.

DPA staff themselves raise the issue of the enforceability of the authorities' decisions, which is related to their limited competence to ensure the implementation of decisions, including illegal data processing by public administrations. The lack of human and financial resources hinders the practical working of remedies and undermines the quality of their work, according to the representatives of the national DPAs.

Professionals as well as victims lack awareness of data protection violations, but various EU Member States also offer a number of examples of good practice in awareness-raising programmes.

FRA opinions

Data protection authorities, the main actors protecting data protection rights, play a crucial role in processing the overwhelming majority of data protection complaints. Further action is needed to ensure that access to DPAs is effective in practice.

The independence of DPAs must be strengthened through a reform of EU legislation. DPAs should have enhanced powers and competences, supported by adequate financial and human resources, including diverse and qualified professionals, such as trained information technology specialists and qualified lawyers.

The European Parliament and the Council of the European Union are proposing a regulation to protect individuals with regard to the processing of personal data and on the free movement of such data. This General Data Protection Regulation seeks to harmonise data protection legislation, and strengthen the ability of DPAs to remedy violations.

Data protection strengthening could include safeguards for effective enforcement of their decisions and reasonable length of procedures (see also in the specific context of non-discrimination the 2012 FRA report on Access to justice in cases of discrimination in the EU*). This would enable DPAs to remain the preferred point of access for data protection violations, while streamlining the existing remedy avenues and decreasing overall costs, delays and formalities (see 2012* FRA Opinion on the proposed data protection reform package*).*

To strengthen their authority and credibility, DPAs should play an important role in the enforcement of the data protection system, by having the power to either issue sanctions or initiate procedures that can lead to sanctions (see also the 2010 FRA report on Data protection in the European Union: the role of national data protection authorities*).*

This opinion is in line with the findings in the context of other non-judicial bodies, such as equality bodies, as highlighted in the 2013 FRA Opinion on the EU equality directives (p. 3):

"The degree to which complaints procedures fulfil their role of repairing damage done and acting as a deterrent for perpetrators depends on whether dispute settlement bodies are able to issue effective, proportionate and dissuasive sanctions" *and* "allowing civil society organisations, including equality bodies, to bring claims to court or conduct investigations [...] could help facilitate enforcement".

Data protection authorities are encouraged to be more transparent as well as communicate effectively with the general public, providing necessary information and easing access to remedies in practice. In addition, as highlighted by the 2010 FRA report on the role of national data protection authorities in the EU, DPAs "should promote closer cooperation and synergy with other guardians of fundamental rights [...] in the emerging fundamental architecture of the EU" (p. 8). *Such steps would improve the image of DPAs, their perceived effectiveness and independence, and the trust of the general public.*

Victims lack awareness of data protection violations and of available remedies. These findings from the FRA fieldwork confirm existing FRA research conclusions.

As recognised by the 2010 FRA report on Data protection in the European Union*, awareness-raising on data protection legislation is an important task for relevant institutions, such as national DPAs. A similar lack of awareness was highlighted in the 2012 FRA report on* Access to justice in cases of discrimination *and the 2013 FRA Opinion*

on the EU equality directives, in relation to EU non-discrimination legislation. From the general public to judges, awareness-raising measures are needed. Knowledge about support organisations to which complainants can turn when lodging data protection complaints needs to be significantly enhanced throughout the EU.

The EU could promote and possibly financially support awareness-raising campaigns at EU Member State level. To raise national practitioners' awareness of data protection rules, the FRA, together with the Council of Europe and the European Court of Human Rights, prepared a Handbook on European data protection law. EU Member States could consider taking the necessary steps to increase the public's awareness of the existence and functioning of available complaint mechanisms, in particular DPAs. In addition, DPAs should pay particular attention to cultivating their public profile as independent guardians of the fundamental right to data protection, and should enhance their awareness-raising activities on data protection.

4.3. Obstacles related to the role of the judiciary in effectively remedying data protection violations

In every EU Member State, individuals can initiate judicial proceedings to remedy data protection violations. Once judicial proceedings are initiated, there is then a wide range of possible outcomes depending on the severity of the violation and the type of judicial proceedings initiated (civil and administrative or criminal).

Because it was difficult to find judges to interview across the 16 EU Member States, the social fieldwork does not distinguish between civil and administrative proceedings and criminal proceedings. It does, however, detail two trends across the Member States which influence the effectiveness of judicial proceedings. The fieldwork indicates that very few data protection cases are initiated, so judges lack skills and experience in the data protection field. This also leads to data protection issues being marginalised; they are not seen as a priority when it comes to training and awareness-raising programmes.

The lack of information is also related to knowledge about laws and jurisprudence about data protection, including the application of the legislation (see, for example, the information collected in Austria, the Czech Republic, Finland, France, Greece, Hungary, Latvia, the Netherlands, Poland, Romania and the United Kingdom). This is made worse because the existing laws are often complex and not easy for most of the subjects of data protection violations to comprehend. They can be hard for the legal professionals to understand as well, particularly for those with less experience or non-specialists.

"One reason why these things, which are comparatively rare, become known to courts is that perhaps violations of privacy rights entail non-quantifiable damage or only a quite small and uncertain quantifiable damage. This means that the incentive to use resources on that, I would say, to follow up such materially quite minor-seeming breaches of data protection like a spam e-mail or something similar, is extremely modest." (Lawyer, Germany)

The field of legislation is relatively new, as mentioned in different contexts during the interviews in most of the EU Member States. For example, respondents from Greece tended to link the lack of knowledge to the non-existing 'culture' of seeking redress for data protection violations. The judges interviewed in Germany and the United Kingdom highlighted that very few cases are brought before the courts. On the one hand, this means that the legislation has not been fully clarified in practice; on the other hand, it prevents the victims from considering that the violations they have faced are serious enough to pursue and undergo lengthy court proceedings.

One of the DPA staff in Spain suggested that those responsible for data processing by public and private bodies could draw up standard codes, and so could the organisations in which they gather, through sectoral agreements, administrative agreements or company decisions. Standard codes detail the organisational conditions, the performance system, the applicable procedures, the environmental safety measures, the existing programmes or equipment and the obligations of those involved in the treatment and use of personal information, as well as guarantees in their field for the full enjoyment by citizens of their rights with full respect for the principles and provisions of the Organic Law for Data Protection and its developing rules.

Judges and practising lawyers in Austria, Bulgaria, the Czech Republic, France, Germany, Greece, Italy, Latvia, the Netherlands, Portugal and Romania confirmed that very few complaints concerning data protection were recorded, and, consequently, very few court cases took place.

Because few proceedings are initiated, judges do not gain expertise in the area and have limited knowledge of and sensitivity to data protection issues. The lack of specialisation of the judges was raised as a serious issue by the respondents from most countries. The lawyers interviewed maintained that to a certain extent they were relied upon to 'inform' the judges on data protection issues in the course of the procedures. This makes the process troublesome. The judges interviewed were also of the opinion that the judiciary lacked knowledge and expertise. They pointed out that it was difficult to

stay informed about data protection issues when there are almost no cases taking place (mentioned during the interviews in the Czech Republic, France, Hungary, Italy, the Netherlands, Portugal and the United Kingdom).

"No, they don't really have any expert knowledge, it is not common to judge cases like that, the professional expertise of judges is a problem in this respect." (Judge, Czech Republic)

"Ordinary court judges know nothing specifically about the law, and have no specialist knowledge, unlike the tribunal." (Judge, United Kingdom)

"If you're doing a subject access case or any data protection case, in the county court – the overwhelming likelihood is that it will be that judge's first case in data protection, even if they're experienced. If you're in the High Court, you might be in front of someone who has dealt with data protection at some point." (Lawyer, United Kingdom)

"I know the issue of personal data very well, but I didn't think that the judge would know it so little. They have difficulty understanding that the name, surname, phone number, but also the image of the individual from video surveillance, voice and call-recording constitute personal data. They do not recognise the presence of personal data. It is a shame that in some cases, before the courts dealing with civil press offences, we never had a decision ruling on the subject. The judges consider that personal data that is not digital cannot be considered as such. So it is not worth the cost for lawyers to appeal to legal theory when we won the case on the image rights." (Lawyer, France)

"I can only speak for civil court cases, in which there is no apparent expertise manifesting itself. Considering the low number of [protection violations] cases we get – I mentioned four or five cases over the last five years, which means about one case per year – then there are just too few to be actively involved in this matter." (Judge, Netherlands)

"Expertise on the theme is low precisely because, for a judge who covers a broad variety of themes, data protection is relatively new." (Lawyer, Italy)

"We end up by lacking the necessary experience, I think, because we also do not have enough cases. That is in my opinion the big issue. Awareness-raising among magistrates, within the justice system – law enforcement agents, lawyers, judges, prosecutors – you still do not see the citizen putting pressure on the system in these cases." (Judge, Portugal)

"I don't think that there is any judge who would specialise in that. They [the cases] would not supply enough cases for a judiciary branch." (Judge, Hungary)

As mentioned previously, some of the respondents doubted that judicial specialisation in the area of data protection is needed, because so few cases are brought before the courts. Training or support that would help improve the expertise of judges (including training on the law and information technology) is in short supply, and there is limited motivation for training (as noted by the respondents in Bulgaria, the Czech Republic, Hungary and the Netherlands). In most of the EU Member States researched, data protection is not considered an important area. As a consequence, improving the specialisation and development of judicial expertise in this area is not prioritised.

"For one case per year you simply do not follow an expensive course. […] Nobody will sign up [for such courses], simply because no one ever gets such [data protection violation] cases." (Judge, Netherlands)

"I am sure there were a number of training programmes in the area of civil courts and the protection of the individual. On the other hand, our area is a little neglected. But again, the option is there. I think there are ways we can increase our level of expertise, knowledge: you can read judgments and the practice of the EU courts. If you're interested, the options are there. I have to say that in today's world of law, ordinary people simply cannot concentrate on a ridiculous number of areas and keep in touch with all changes." (Judge, Czech Republic)

The Italian judges suggested four potential measures that could improve judicial proceedings. The first measure is to create information points that offer information on the rights of data subjects, as provided for in the data protection act. A second measure is to simplify proceedings; this could make redress mechanisms more accessible. Another suggestion addresses a collective project to gather information, develop investigations and promote class action. Finally, access to databases containing legal texts and decisions of DPAs, national and European courts would be good practice, increasing awareness and providing access to victims of data protection violations.

Too few judges are specialised in the data protection area. Judges and practising lawyers pointed out that few cases reached courts and that there were too few professionals in the field. They highlighted the need for training, better knowledge of the legislation and specialisation in the area.

Conclusions

A number of ways forward exist to improve the availability and quality of remedies available to victims of data protection violations in the EU. The EU, its Member States and individual DPAs all have a role to play in developing the current approach to providing remedy.

The EU institutions play a particularly important role in this area. The European Commission has proposed a draft regulation setting out a general EU framework for data protection, which seeks to harmonise data protection legislation and to strengthen the ability of DPAs to remedy violations. It is essential that DPAs be fully independent from external control, particularly as they have to address data protection violations by the state. The allocation of funds, and subsequent decisions on how to spend them, and their recruitment procedures must both be independent. It is also essential that they have proper procedures, sufficient powers and adequate resources, including qualified professionals to make use of these procedures and powers. This also applies to civil society organisations. The EU should ensure that civil society organisations and independent bodies in a position to assist victims in seeking redress in the area of data protection are sufficiently funded. To further enhance the ability of victims to bring claims, the EU should consider further relaxing rules on legal standing. Enabling organisations to lodge a complaint before a supervisory authority or a court, while acting in the public interest, would open the door to a much wider collective action.

EU Member States can also improve existing data protection mechanisms by taking the necessary steps to increase the general public's awareness of the available complaint mechanisms and how they work. They should particularly highlight civil society organisations that offer support to complainants. Member States should also strengthen the professional competence of judges and lawyers in the area of data protection, providing training sessions and placing added emphasis on data protection issues in the legal curriculum. In addition to ensuring the quality of – and access to – legal representation, this would usefully reduce the length of proceedings, which the fieldwork highlighted as a barrier to those seeking remedies.

Data protection authorities are also a crucial part of the EU fundamental rights landscape, and it is important that those seeking remedies recognise them as such. Data protection authorities are independent guardians of the fundamental right to data protection. They should pay particular attention to cultivating their public profile and focus on raising awareness of their existence and role. They should also seek closer cooperation with other guardians of fundamental rights such as equality bodies, human rights institutions and civil society organisations.

The recommendations for ways forward reinforce those proposed in previous FRA reports. These include the FRA report on *The independence of data protection authorities in the EU* and their funding and staffing; the 2010 FRA report on *Data Protection in the European Union*; and the 2012 FRA Opinion on the proposed data protection reform package. Dealing with access to justice in particular, the finding of this report mirror those found in the 2011 FRA report on *Access to justice in Europe: an overview of challenges and opportunities*; and the 2012 FRA report on *Access to justice in cases of discrimination in the EU*.

These proposed actions, if taken by the EU, Member States and DPAs, would alleviate the problems highlighted by the key findings of the social fieldwork.

References

All hyperlinks were accessed on 30 November 2013.

Council of Europe (CoE) (1981), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981 (Convention 108), available at: www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

CoE (2001), Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, CETS. No. 181, 2001, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm.

Council of the European Union (2008), Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L 350.

Court of Justice of the European Union (CJEU), C-518/07, *European Commission v. Germany*, judgment of 9 March 2010.

CJEU, Joined Cases C-402/05 P and C-415/05 P, *Kadiand Al Barakaat International Foundation v. Council and Commission*, 3 September 2008.

Denmark, Act No. 430 of 1 June 1994 on information-databases of the mass media (*Lov nr 430 af 1 Juni 1994 om massemediers informationsdatabaser*), available in Danish at: www.retsinformation.dk/forms/r0710.aspx?id=59461.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281 (*Data Protection Directive*), available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

European Commission (2011) *Attitudes on data protection and electronic identity in the European Union*, Special Eurobarometer 359, Brussels, TNS Opinion & Social.

European Commission (2012a), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

European Commission (2012b), *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, COM(2012) 10 final, Brussels, 25 January 2012, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf.

European Commission (2012c), *Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, Commission Staff Working Paper, SEC(2012) 72 final, Brussels, 25 January 2012.

European Commission (2012d), *Cyber security*, Special Eurobarometer 390, Brussels, TNS Opinion & Social available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

European Commission (2013a), *Proposal for a Council decision on the conclusion of the Agreement between the European Union and the Russian Federation on drug precursors*, COM(2013) 4 final, Brussels, 21 January 2013, Annex II – Data protection definitions and principles, p. 15, available at: http://ec.europa.eu/taxation_customs/resources/documents/common/legislation/proposals/customs/com(2013)4_en.pdf.

European Commission (2013b), Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law, OJ L 201, 26 July 2013, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32013H0396:EN:NOT.

European Commission (2013c), *Towards a European horizontal framework for collective redress*, COM(2013) 401/2, Brussels, available at: http://ec.europa.eu/justice/civil/files/com_2013_401_en.pdf.

European Centre for Disease Prevention and Control (ECDC) (2013), *ECDC mission report – joint technical mission: HIV in Greece 28–29 May 2012*, Stockholm,

ECDC, available at: http://ecdc.europa.eu/en/publications/publications/hiv-joint-technical%20mission-hiv-in-greece.pdf.

European Court of Human Rights (ECtHR), *I. v. Finland*, No. 20511/03, 3 April 2007.

ECtHR, *Leander v. Sweden*, Series A No. 116, 26 March 1987.

ECtHR, *Lyanova and Aliyeva v. Russia*, Nos. 12713/02 and 28440/03, 2 October 2008.

ECtHR, *Kennedy v. the United Kingdom*, No. 26839/05, 18 May 2010.

ECtHR, *Peck v. the United Kingdom*, No. 44647/98, 28 January 2003.

ECtHR, *Rotaru v. Romania*, No. 28341/95, 4 May 2000.

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*, Luxembourg, Publications Office of the European Union (Publications Office), available at: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf.

FRA (2011a), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office, available at: http://fra.europa.eu/en/publication/2011/access-justice-europe-overview-challenges-and-opportunities.

FRA (2011b), *Fundamental rights: challenges and achievements in 2011*, Luxembourg, Publications Office, available at: http://fra.europa.eu/sites/default/files/fra_uploads/2211-FRA-2012_Annual-Report-2011_EN.pdf.

FRA (2012a), *European Union data protection reform: new fundamental rights guarantees*, FRA Symposium Report, Vienna, 10 May 2012, available at: http://fra.europa.eu/sites/default/files/fra_uploads/2280-FRA-Symposium-data-protection-2012.pdf.

FRA (2012b), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*, FRA Opinion 2/2012, Vienna, 1 October 2012, available at: http://fra.europa.eu/en/opinion/2012/fra-opinion-proposed-eu-data-protection-reform-package.

FRA (2012c), *Access to justice in cases of discrimination in the EU: steps to further equality*, Luxembourg, Publications Office, available at: http://fra.europa.eu/en/publication/2012/access-justice-cases-discrimination-eu-steps-further-equality

FRA (2013), *Opinion of the European Union Agency for Fundamental Rights on the situation of equality in the European Union 10 years on from initial implementation of the equality directives*, FRA Opinion 1/2013, Vienna, 1 October 2013, available at: http://fra.europa.eu/sites/default/files/fra-2013_opinion-eu-equality-directives.pdf.

FRA (2014 forthcoming), *Independence of data protection authorities in the EU. Data protection authorities' funding and staffing*, Luxembourg, Publications Office.

FRA and Council of Europe (2014), *Handbook on European data protection law,* Luxembourg, Publications Office.

Germany (1999), Trade Licencing Act (*Gewerbeordnung*), 1999, available at: www.gesetze-im-internet.de/bundesrecht/gewo/gesamt.pdf.

Hungary (2011), Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Privacy Act), available at: www.naih.hu/act-cxii-of-2011---privacy-act--.html.

Italy, Government (2010), *Annual Report to the Parliament for the year 2010*, Rome, available at: www.commissioneaccesso.it.

Latvia (2005), Law on Compensations for Loss Caused by State Administrative Institutions (*Valsts pārvaldes iestāžu nodarīto zaudējumu atlīdzināšanas likums*), 2005.

National Authority for Data Protection and Freedom of Information (NAIH) (2013), *Annual report of the National Authority for Data Protection and Freedom of Information*, Budapest, NAIH.

Parliamentary and Health service Ombudsman (2011), *A breach of confidence – A report by the Parliamentary Ombudsman on an investigation of a complaint about HM Revenue & Customs, the Child Support Agency and the Department for Work and pensions*, London, The Stationery Office, available at: www.ombudsman.org.uk/__data/assets/pdf_file/0012/6411/PHSO-0108-HC-709-report-final-web-11012011.pdf.

Portugal Communications Authority (*Autoridade Nacional de Comunicações*) 2011, Supervisão e Acompanhamento De Mercado, available at: www.anacom.pt/streaming/Supervisao_Acompanhamento_Mercado_relaregulacaosuperv_2010web.pdf?contentId=1101646&field=ATTACHED_FILE.

Annex: Information about the fieldwork and interviewees

Description of interviewees

Table A1: Numbers of interviewees and participants in focus group discussions

	Number of interviewees			Number of participants in focus groups or interviews		
	Complainants	Non-complainants	Judges/ prosecutors	DPA staff	Intermediaries	Practising lawyers
Minimum planned	*30–40*		*6*	*6*	*6*	*6*
Austria	7	6	5	2	7	8
Bulgaria	16	14	8	6	2	3
Czech Republic	4	6	5	10	6	6
Finland	24	6	6	8	6	6
France	25	9	5	6	7	8
Germany	20	6	5	6	5	4
Greece	16	15	4	7	7	5
Hungary	13	19	6	9	6	5
Italy	2	9	6	7	7	7
Latvia	5	2	2	5	5	4
Netherlands	24	9	7	6	6	5
Poland	15	15	6	8	8	6
Portugal	7	7	6	2	3	4
Romania	4	2	3	0	6	3
Spain	11	3	4	5	6	6
United Kingdom	28	2	6	10	9	4
Total	**351**		**84**	**97**	**96**	**84**

Source: FRA, 2013

As has been mentioned, the final sample includes more **complainants** (221) than **non-complainants** (130). More men than women were interviewed; nearly two out of three complainants were men, with an equal share of men and women among the non-complainants. The majority of the interviewees of these target groups are aged between 25 and 60, and are resident in capital cities, main towns or other urban areas (with a few exceptions living outside these areas). The fieldwork covered a wide and diverse range of the types and areas of the data protection violations faced by the complainants and non-complainants in the last three years before the research in all the 16 EU Member States. It also covered a variety of possible redress mechanisms.

The main criteria for selecting the **judges** and the **lawyers** were related to their professional experience. They should have direct experience with different types of redress mechanisms in the field of data protection during the previous three years: civil court or tribunal; criminal court or tribunal; administrative court or tribunal; alternative dispute settlement procedure.

The fieldwork shows that most of the **judges** interviewed have more than 10 years of experience in the court system; approximately one in three have under 10 years of experience. The average number of cases dealt with in the last three years ranged significantly from just a few cases to tens or hundreds. The judges from Germany, Hungary and Spain referred to the largest number of cases, followed by representatives from Bulgaria and the United Kingdom. This included some with very limited experience. The judges from the Czech Republic, France, Latvia, Portugal and

Romania had handled very few cases of data protection violations; some had handled only one. The majority of judges interviewed in all the 16 EU Member States had professional experience in the administrative courts and tribunals. They also mentioned experience in the criminal and civil courts, but in none of the countries covered was a judge available with experience of alternative dispute settlement procedures. Moreover, in some of the Member States, the judges interviewed had professional experience of only one type of redress mechanism: in Greece, only the administrative courts; in Hungary, only the civil courts. Additionally, more of the judges were men than women.

Of the **practising lawyers** interviewed, approximately one in four had up to five years of experience in the data protection area, one in three had from six to 10 years, and one in four had over 11 years of experience in the field. Their professional experience was mostly in alternative dispute settlement procedures and especially complaints to the national DPAs. Some of the lawyers had experience in the field of administrative and civil courts. The least professional experience was in criminal trials. Two thirds of the lawyers interviewed were men.

Almost half of **national DPA representatives** worked in the area of data protection or directly with redress mechanisms in the data protection field for up to five years, and over one third of them had been working in the field between six and 10 years. One fifth claimed to have over 11 years of experience. Among the DPA representatives, more women than men were interviewed.

The **intermediaries** are representatives of civil society organisations that provide support to the subjects of data protection violations. Most of these interviewees represented NGOs, associations or other organisations. Very few were from private companies. The other organisations represented include trade unions, representation for employees, political organisations, national human rights institutions and other associations or organisations that deal with data protection cases from time to time. For all of these organisations, the area of data protection only comprises a small portion of their work. Most of the organisations provide legal counselling services for the subjects of data protection violations. Most of the intermediaries contacted during the research had experience with non-judicial procedures, particularly complaints lodged to the national DPAs. No intermediary interviewed in Hungary, Latvia or Spain had experience with judicial proceedings. Next most commonly mentioned were activities related to the administrative institutions procedures, followed by involvement in the proceedings of the civil courts. Criminal proceedings were again the least frequently mentioned. When lawyers represented intermediary organisations, their opinions and perceptions were analysed as those of intermediaries and not of the group of practising lawyers. In comparison with the other target groups, the sample of intermediaries is gender balanced.

Accessing interviewees

Although a representative sample is not possible for a limited number of respondents in qualitative research, the selection criteria for each target group were designed to ensure variety, and were applied in all the countries researched, where possible. Referrals of potential interviewees were sought through a wide range of channels: national DPAs,[61] other state authorities, possible intermediaries and professional associations (e.g. those of judges and lawyers) as well as by direct mailing. Attempts to create a pool of interviewees targeted specific websites, using online networks, social media, blogs, newsletters, advertisements in local media, etc.

There were challenges in recruiting appropriate individuals in nearly all countries covered in the fieldwork. Only in two countries, namely Germany and the United Kingdom, did the samples reach the desired size, and even there relevant adjustments were made during the fieldwork.

The evidence indicated differences between countries in terms of the mechanisms available, the professionals involved and their experience in dealing with redress in the area of data protection.

The target number of complainants was 14 or more. Of the 16 EU Member States covered by the research, just over half provided this many (Bulgaria, Finland, France, Germany, Greece, Hungary, the Netherlands, Poland and the United Kingdom). There were much lower numbers of complainant interviews elsewhere (two in Italy, four each in Romania and the Czech Republic, five in Latvia and seven in Portugal), with the exception of Spain, which provided a sample of 11 complainants. The group that was hardest to reach was non-complainants; most countries were unable to recruit the target number of respondents. In some countries, more complainants were interviewed to compensate for this (e.g. 24 in Finland, 25 in France and 28 in the United Kingdom).

It was difficult to find interviewees who had contacted any institution or organisation while considering using the redress mechanisms and had then refrained from it. On the one hand, most of the institutions or organisations do not have any information about persons who seek advice but then decide not to complain. On the

61 The research benefited in the countries where the national DPAs expressed their cooperation and informed others, as well as supporting to get into contact with other target groups (complainants, judges or intermediaries).

other hand, according to the fieldwork material, a decision to seek redress and initiate the procedure depends strongly on the awareness of the available options for legal redress procedures. The findings suggest that non-complainants appear to have a low awareness of the available redress mechanisms as well. The sample of non-complainants includes individuals who considered complaining and took some practical steps, as well as those who did not consider complaining and so took no further action.

It was also difficult to reach reasonable numbers of experienced[62] judges (only five countries were able to locate the minimum number of judges required for this study) and practising lawyers (almost all countries). This appears to reflect the minor role of data protection within the national judiciary. According to the judges, it is related to the small number of cases in the area (e.g. in Italy and Romania). The lawyers highlighted the absence of legal expertise in the field of data protection. In a few countries, judges and lawyers refused to take part in the research because they had limited experience in the field or considered that the number of relevant cases was too small to provide meaningful information (Bulgaria, the Czech Republic, Germany, Latvia, Portugal and Spain). Some of the lawyers confirmed their limited experience during the interviews.

The main challenges with regard to the intermediaries were related to low numbers of organisations specialising in the data protection area in the countries. In the final sample, organisations differed according to their nature or activities; very few civil society organisations specialised (having solid experience, ensuring permanent specialised services or free of charge services) in the area of data protection.

62 This means experienced with different types of redress mechanisms in the field of data protection in different areas, working in different administrative units of the country and having over three years' experience in the field of data protection.

European Union Agency for Fundamental Rights

Access to data protection remedies in EU Member States

2013 — 59 p. — 21 x 29.7 cm

ISBN 978-92-9239-460-8
doi: 10.2811/69883

A great deal of information on the European Union Agency for Fundamental Rights is available on the Internet.
It can be accessed through the FRA website at fra.europa.eu.

doi:10.2811/69883
TK-01-14-288-EN-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

Technological advances make it ever more important to safeguard the right to personal data, which is enshrined in the Charter of Fundamental Rights of the European Union. Data protection violations arise principally from internet-based activities, direct marketing and video surveillance, perpetrated by, for example, government bodies or financial and health institutions, research by the European Union Fundamental Rights Agency (FRA) shows. Those victimised seek redress primarily to ensure that similar violations do not recur. This FRA socio-legal project, which offers an analysis of the 28 EU Member States' data protection regimes and of interviews with relevant parties in 16 Member States, highlights the challenges people face when seeking such remedies. It finds that only a few are aware of their right to data protection and that there is a lack of legal expertise in the field. Those who do file complaints typically address their national data protection authorities, but these often suffer from a lack of resources and powers. The findings provide evidence to inform and contribute to the European Union's efforts to comprehensively reform and enhance the EU's data protection regime.

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel.: +43 158030-0 – Fax: +43 158030-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Publications Office

ISBN 978-92-9239-460-8