

# Access to data protection remedies in EU Member States

## Summary

*Article 8 of the Charter of Fundamental Rights of the European Union guarantees all individuals in the European Union (EU) the right to the protection of their personal data. It requires that such data be processed fairly for specific purposes. It secures each person's right of access to his or her personal data as well as the right to have such data rectified. It stipulates that an independent authority must regulate compliance with this right. Article 47 secures the right to an effective remedy, including a fair and public hearing within a reasonable timeframe.*

Data protection violations can and do occur almost anywhere: at work, in the supermarket or while on the internet. They can cause emotional distress and damage to one's reputation or relationships.

*"The consequences [of the breach 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."*

(Victim of data protection violation who did not seek a remedy, Germany)

Those who have experienced such violations are entitled to seek a remedy. They may turn to their national data protection authority or other available alternatives to complain or seek redress. Many seek a remedy to prevent similar harm to others or to gain recognition that their rights have been violated. They may, however, be dissuaded from filing a complaint because they fear the proceedings will be too lengthy, complex or costly, particularly if they

require legal representation. They may also fail to find the expertise or advice they need.

This FRA project provides an EU-wide comparative analysis of the remedies available as a means of ensuring individuals' rights in the area of data protection. It focuses on the juncture of two fundamental rights safeguarded 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 (Article 47). The right to an effective remedy is a prerequisite for the effective enforcement and implementation of all other fundamental rights, including data protection. As such, it is important to look at both fundamental rights together.

*"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.'"*

(Victim support organisation representative, Romania)

The FRA legal and social research examines the use and application of data protection remedies as well as the barriers to seeking an effective remedy for a data protection breach. Based on its research evidence, FRA identifies the stumbling blocks and suggests how to remove them, aiming thus to contribute to the ongoing reform of the data protection regime in the EU.

This summary presents the FRA's main research conclusions, which are published in full in *Access to data protection remedies in EU Member States* (see Further information).

## Legal context

The EU Data Protection Directive, or 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, guarantees the availability of data protection remedies in EU Member States by requiring each Member State to set up an independent supervisory authority.

The European Commission, driven by a desire for more effective enforcement of the fundamental right to personal data protection, proposed

a comprehensive reform of the EU’s data protection rules in 2012. The reform package consists of a proposal for a General Data Protection Regulation replacing the 1995 Data Protection Directive and a proposal for a General Data Protection Directive replacing the 2008 Data Protection Framework Decision.

The proposed reform package aims to enhance the independence of national data protection authorities and to strengthen the powers of such authorities to remedy violations.

### Description and categories of interviewees

All of the summary’s quotes are taken from the full report *Access to data protection remedies in EU Member States*. To improve the summary’s readability, FRA has altered the categories of those who gave quotes. The summary refers to the source of a quote as ‘a victim of a data protection violation who did not seek a remedy’,

which appears in the full report under the legal term ‘non-complainant’. Similarly, those victims who did seek a remedy are referred to in the full report as ‘complainants’. FRA also interviewed individuals working at support organisations for data protection violation victims, including groups such as employee organisations, trade unions or complaints organisations. The summary specifies their roles; the full report refers to them as ‘intermediaries’. ‘Lawyers’ and ‘judges’ are referred to as such in both the summary and the full report.

**Table: 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 |
| <i>Minimum planned</i> | 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                  |
| <b>Total</b>           | <b>351</b>             |                  | <b>84</b>          | <b>97</b>  | <b>96</b>      | <b>84</b>          |



## Data collection and coverage

For this research, FRA examined the legal framework on data protection in the 28 EU Member States, analysing laws and rules of procedure to present a comparative analysis of the legal situation on data protection across the EU.

From April to September 2012, qualitative fieldwork was carried out by FRA's multidisciplinary research network, Franet, in 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. More than 700 individuals from six target groups were interviewed or took part in focus groups. These six target groups were: complainants, or victims of data protection violations who sought a remedy; non-complainants such as alleged victims of data protection violations who decided against seeking a remedy; judges; staff of data protection authorities; intermediaries, including staff members of civil society organisations who provide support for the individuals subjected to the data protection violations; and practicing lawyers.

## Key findings and evidence-based advice

Based on its findings, FRA sees concrete possibilities for EU institutions, Member States and mechanisms involved to implement data protection remedies to improve the availability and quality of remedies to victims of data protection violations in the EU. In light of this, FRA suggests several steps to support EU institutions and national policy makers in developing and implementing measures designed to safeguard the protection of personal data and to claim redress in case of violation.

### Knowing one's rights: raise awareness

Greater public awareness of the right to data protection, the nature of violations of this right, redress mechanisms and how to take advantage of them also contribute to the effectiveness of remedies. The public must be able to recognise a data protection violation to pursue a remedy.

This FRA research looked at the different types of violations, who commits them and the impact of those violations on victims. It also examined what motivated victims to seek remedies.

### Data protection violation types

Internet-based activities, direct marketing, and video surveillance through the secret use of CCTV emerge in the fieldwork as the most frequent sources of data protection violations. Government bodies, law enforcement agencies, and financial and health institutions are most often responsible for these violations.

The most frequent data protection violations that were mentioned during the fieldwork refer to internet-based activities. These include social media, online shopping, leakage of personal data from e-shops, email account and databases hacking, identity theft, security breaches, and misuse of personal data by global internet companies. Internet-based activities clearly emerge as a high risk territory from a data protection point of view.

Another prevalent data violation is direct marketing and commercial prospecting without the consent of the recipient, when the personal data is misused either on mobile phones, by emails or by post. Mobile phone operators and debt collectors are often responsible for these violations, the fieldwork suggests. Respondents also note irregular practices such as selling personal data to third parties.

Interviewees often refer to hidden video surveillance at the workplace, in the public sphere or in supermarkets. Several respondents from different countries say they have been confronted with secret surveillance conducted by public authorities with special technology or by secretly installed closed-circuit television. Several data protection authorities, for example in the United Kingdom, have elaborated guidelines on the use of closed-circuit television.

In employer-employee relationships specifically, respondents also mention other alleged data protection violations. These include: collection of employees' personal data, access to personal data stored on employers' computers, use of badging and global positioning systems, discriminatory usage of sensitive personal data collected through surveys or audits, and disclosure of employees' data by employers.

The fieldwork also finds that financial violations are quite common, including breaking into bank accounts or credit card hacking. Despite this, the research identifies only few complainants who say they have suffered financial loss from the violation. In many of those cases, respondents describe the sums involved as minor, relating to telephone calls, postage and the costs of having records accessed and amended.

## Impact on victims

Respondents describe the damage from data protection breaches as psychological and social in nature, such as emotional distress or reputational damage. Participants also, although less frequently, report financial damages.

Those who have experienced data protection violations seek redress for many reasons, such as rectification or deletion of personal data or sanctions against violators. Respondents say they seek to protect others by preventing future violations and to gain recognition that a violation has taken place.

When asked what damage the data protection violation has caused them, the complainants and non-complainants most commonly describe it in psychological or social terms. They focus either on their emotions or on the harm it has done to their relationships or reputation. They speak of varying degrees of emotional distress, offence and insecurity, such as feelings of persecution or of being under surveillance, even helplessness. They describe damage to their professional or personal reputation, loss of trust and other forms of moral damage, as FRA fieldwork research highlighted in, for example, Austria, Bulgaria, Germany, Greece, Hungary, Italy, Latvia, the Netherlands, Poland and Spain. One Spanish complainant characterises one aspect of this feeling as “impotence regarding an abuse of power”.

*“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.”*

(Victim of data protection violation who sought a remedy, Greece)

Interviewees in the Czech Republic, Italy, the Netherlands, Portugal and Romania note damage from violations in the area of employment, such as disciplinary procedures, suspensions and/or termination of employment or risk of dismissal. In some of these cases, the damages refer to financial losses, 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.

Some respondents seek redress to resolve principally their personal situation. A much greater proportion aim to prevent violations to others in future, gaining recognition for, or putting a stop to, the violation or sanctioning the perpetrator. Financial compensation is not a prevalent reason for seeking redress. Respondents most commonly mention ‘prevention of future breaches of rights’, ‘awareness raising’, ‘stopping the wrong practice’, ‘standing up for fundamental rights’, ‘teaching a lesson to [the authorities concerned]’, ‘obtaining an acknowledgement of the breach from a competent authority’ or ‘sanctioning of the perpetrator’.

While respondents highlight a lack of awareness of the problem of data protection violations among professionals as well as victims, various EU Member States also have awareness-raising programmes.

### FRA opinion

*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 data protection authorities. 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 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 data protection authorities. In addition, data protection authorities 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.*

## Seeking remedy: strengthen data protection authorities

For those seeking redress for data protection violations, data protection authorities proved the most popular, and in many cases the only relevant, avenue to seek redress. To meet this demand, they need to be empowered to provide a robust and comprehensive service.

The 1995 Data Protection Directive sets out the powers of data protection authorities, granting them the power to investigate and intervene to prevent violations. They play a major role in remedying data protection violations, often acting as the first point of contact for victims of such violations. This role is often recognised by national courts; in Finland, for instance, the prosecutors and courts are obliged to provide the data protection authority with an opportunity to be heard in cases which handle conduct contrary to the Finnish Personal Data Act.

## Enhancing the role of data protection authorities

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.

Data protection authority 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 data protection authorities.

Data protection authorities can issue orders to rectify data protection violations or impose fines, although their powers to remedy such violations, and the extent to which they use them, vary greatly across the EU Member States. These powers include formal warnings, specific orders, injunctions, revocation of licences fines, other monetary sanctions or a referral of the case either to the relevant Member State's courts or public prosecutor.

*"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 is 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."*  
(Data protection authority staff, Austria)

Judicial authorities in the majority of EU Member States can impose criminal sanctions in the form of a fine or imprisonment. The range of sentence duration and the fine's amount vary across the EU Member States. For some respondents in the social fieldwork, concretely judges in Greece, the severity of sanctions contributes to the effectiveness of judicial procedures.

Although the data protection authorities typically have a number of measures at their disposal, they most commonly issue a fine or pecuniary sanction in the event of a data protection violation, as reported in 19 EU Member States. National legislation often sets out the amount of the fine imposed, 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 for cases in which numerous violations have been committed.

*"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."*  
(Data protection authority staff, Germany)

The adoption of the proposed European Commission regulation would enshrine in EU law the power of these authorities to impose administrative sanctions, namely fines and other monetary sanctions. Although the majority of data protection authorities already have this power, FRA findings show, 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.

## Seeking redress through data protection authorities

The majority of the complainants in the 16 EU Member States covered by the research choose to seek redress through the national data protection authority. 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 data protection authority 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; as well as the limited availability of other procedures.

The complainants surveyed were more reluctant to initiate court proceedings due to 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.

*“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.”*  
(Victim of data protection violation who sought a remedy, Latvia)

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 say they lack information. The second group, a minority of ‘well-informed’ interviewees, say they have enough information because of their professional background, typically legal, or previous experience.

### FRA opinion

*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 data protection authorities is effective in practice.*

*The independence of data protection authorities must be strengthened through a reform of EU legislation. Data protection authorities 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 to strengthen the ability of data protection authorities 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 data protection authorities 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 the 2012 FRA Opinion on the proposed data protection reform package).*

*To strengthen their authority and credibility, data protection authorities 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 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, data protection authorities “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 data protection authorities, their perceived effectiveness and independence, and the trust of the general public.*

## Enlisting support: enhance the role of civil society organisations

Civil society organisations emerged in the fieldwork as an important source of information, advice, legal assistance and representation. They provide a valuable addition to the statutory data protection framework. They also create awareness and publicise data protection issues and possible remedies. There are, however, too few such organisations – a factor that limits people’s access to remedies in practice.

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.

*“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 class-action instrument, in the case where the issue can be of interest to a plurality of individuals.”*

(Victim support organisation representative, Italy)

FRA fieldwork in the 16 EU Member States faced difficulty finding potential interviewees representing civil society organisations, or intermediaries. In most countries, it was a challenge to find representatives from organisations that specifically deal with data protection issues, provide support to the victims of violations or have extensive experience in the area.

The intermediaries interviewed during the fieldwork say they mainly provide advice and information to individuals, who have experienced data protection violations, on their rights and the remedies available. They assist individuals with their complaints. Other activities mentioned by research respondents include education, research and training. Some highlight awareness-raising work through media campaigns, articles and publications, as well as monitoring and lobbying work.

*“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.”*

(Victim support organisation representative, Bulgaria)

### 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.*

*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.*

## Breaking down barriers: reduce costs and ease the burden of proof

The FRA research sought to identify the factors that keep victims of data protection violations from seeking a remedy. In addition to a lack of expert advice and support, it uncovered a number of barriers, including costs, the excessive length of proceedings and the difficulties of satisfying burden of proof requirements, particularly for internet-related violations.

Respondents consider 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.

Complainants, intermediaries and the practicing 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.

Somewhat predictably, individuals subjected to violations tend to prefer remedies that do not involve costs. The fieldwork findings from most of the 16 EU Member States researched reveal that costs and cost-risk were among the major concerns for individuals when deciding to initiate or continue their cases.

The cost of legal representation, for example, often dissuaded victims of data protection violations from pursuing complaints. 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 of remedies. Legal aid and other means that render redress mechanisms cost-free help to make these mechanisms more accessible to a greater number of people. Fieldwork findings indicate limited access to redress mechanisms due to the limitation of legal aid.

*“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 to 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. Self-representation may not be preferable, however, owing to the complexities of this area of law. Nevertheless, it does give complainants, who might not otherwise have done so, the opportunity to bring claims.

The high cost of judicial procedures is a related concern. It often keeps complainants from approaching the courts, even if by winning the case they could get compensation. Respondents in many of the EU Member States researched consider high procedural costs in civil legal proceedings, including court fees, to be a problem; this is the case, for example, in Austria, France, Germany, Greece, Hungary, Italy, the Netherlands, Poland, Portugal, Spain and the United Kingdom.

*“In civil procedures you’ve 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)*

Another barrier to the pursuit of claims is the burden of proof. Most of the complainants interviewed from the 16 EU Member States covered by the fieldwork mention difficulties in providing sufficient and complete evidence. Complainants interviewed in the Czech Republic, Greece, Latvia, Portugal, Romania and Spain point to the burden of proof as a barrier in seeking remedies in the area of data protection. The problems focus on the difficulty in proving the data protection violations, mainly regarding internet-based activities and several practical obstacles related to obtaining evidence in the specific field of data protection. The lawyers and intermediaries interviewed share this opinion, whereas judges, for example in Portugal and Romania, consider the burden of proof as acceptable.

### FRA opinion

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

## Providing advice: enhance legal expertise on data protection

The research reveals a lack of expertise in the legal profession in the field of data protection. In addition to the lengthy, complex, costly and time-consuming procedures, the paucity of sound expert advice keeps many victims from pursuing a remedy. Building greater professional competence among lawyers and judges in data protection would make such needed expertise available and speed up decision making while cutting down on lengthy proceedings.

Legal professionals themselves point out that there are too few professionals in the field and that few cases reach the courts, comments which chime with the difficulty the project had in finding judges and lawyers to interview for the fieldwork.

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

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 keep them from seeking redress for data protection violations.

Individuals in every EU Member State can initiate judicial proceedings to remedy data protection violations. Once judicial proceedings are launched, there are a number of possible outcomes depending on the severity of the violation and the type of judicial proceedings initiated – civil and administrative, or penal.

*“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)

The social fieldwork points to two trends across EU Member States, which have consequences for the effectiveness of judicial proceedings. Very few data protection cases are initiated and, as a result, judges lack skills and experience in the data protection field. This, in turn, leads to the marginalisation of data protection issues, which are not seen as a priority when it comes to training and awareness-raising programmes.

### 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 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.*

## Conclusions

There are a number of ways forward 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 data protection authorities all have a role to play in developing the current approach to providing remedy.

The role of EU institutions is particularly important in this area. The European Commission has proposed a draft regulation setting out a general EU framework for data protection. The proposed framework seeks to harmonise data protection legislation across EU Member States and to strengthen the ability of national data protection authorities to remedy violations. It is essential that data protection authorities are independent from external control, both for allocating and spending funds and for recruiting personnel. Such independence is particularly important since data protection authorities also have to address data protection violations by the state. Moreover, they must be equipped with proper procedures, sufficient powers and adequate resources, including qualified professionals to make use of these procedures and powers.

The EU should aim at increasing funding for civil society organisations and independent bodies in a position to assist victims in seeking redress in the area of data protection. To enhance the ability of victims to bring claims, the EU should consider further relaxing legal standing rules to enable

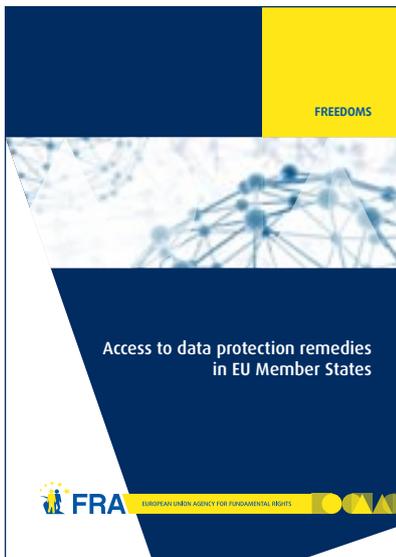
organisations acting in the public interest to lodge a complaint and to open the door to collective action.

EU Member States can help improve existing data protection mechanisms by taking the necessary steps to increase the general public's awareness of the existence and functioning of the available complaint mechanisms for data protection breaches and of civil society organisations that offer support to complainants. Member States should also take action to 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 help 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; it is important that those seeking remedies recognise them as such. Data protection authorities should focus awareness of their existence and role, cultivating their public profile as independent guardians of the fundamental right to data protection. They should also seek closer cooperation with other guardians of fundamental rights such as equality bodies, human rights institutions and civil society organisations.







The full report, *Access to data protection remedies in EU Member States*, examines the nature of data protection violations and highlights the obstacles victims of such violations face when seeking redress. 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, examines 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 Commission's efforts to comprehensively reform and enhance the EU's data protection regime.

## Further information:

For the full FRA report – *Access to data protection remedies in EU Member States* – see <http://fra.europa.eu/en/publication/2013/access-data-protection-remedies-eu-member-states>

An overview of FRA activities on data protection is available at: <http://fra.europa.eu/en/theme/data-protection-privacy>

This summary is also available in French and German. Further translations will be published in 2014, including Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, Greek, Hungarian, Italian, Latvian, Lithuanian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish.



Publications Office

© European Union Agency for Fundamental Rights, 2013  
Photo: © SXC

## FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Schwarzenbergplatz 11 – 1040 Vienna – Austria  
Tel: +43 158030-0 – Fax: +43 158030-699  
[fra.europa.eu](http://fra.europa.eu) – [info@fra.europa.eu](mailto:info@fra.europa.eu)  
[facebook.com/fundamentalrights](https://www.facebook.com/fundamentalrights)  
[linkedin.com/company/eu-fundamental-rights-agency](https://www.linkedin.com/company/eu-fundamental-rights-agency)  
[twitter.com/EURightsAgency](https://twitter.com/EURightsAgency)



TK-01-13-752-EN-C  
doi:10.2811/52756