

Chapter 2

The Effectiveness of Redress Mechanisms.

Case study—Poland

Dorota Głowacka and Beata Konieczna

2.1 Redress Mechanisms Research Study—General Remarks

This article is a result of the national study conducted within the project “Data protection: redress mechanisms and their use”¹ run by the European Union Agency for Fundamental Rights (“FRA”) within its FRANET multidisciplinary research network.² The aim of the project is a comparative overview and analysis of existing procedures and the legal consequences of data protection violations in the EU Member States. The FRA’s previous engagement in data protection related research—such as the report on “Data Protection in the European Union: the role of National Data Protection Authorities”³ as well the special Eurobarometer survey on attitudes towards data protection in the EU⁴—highlighted that redress mechanisms in the area of data protection, even though usually available, are not widely used. The Eurobarometer survey revealed, for example, that only 33 % of Europeans were aware of the existence and competences of the national data protection authority.

The amount of information available at the EU level is still insufficient to fully understand the poor use of redress mechanisms revealed by these researches. The FRA project attempts, therefore, to provide insight into why the existing redress measures in different EU Member States are not applied to their full extent. The answer to this question is particularly important with regard to the planned EU data protection reform, which may bring some innovation in this area compared to the

¹ European Union Agency for Fundamental Rights.

² FRANET is composed of National Focal Points in each EU Member State and Croatia, the aim of this network is to provide the Agency with comparable socio-legal data on fundamental rights issues to facilitate the FRA’s comparative analyses at EU level.

³ European Union Agency for Fundamental Rights (2010).

⁴ Special Eurobarometer 359 (2011).

D. Głowacka (✉)
Zgoda 11, 00-018 Warsaw, Poland
e-mail: d.glowacka@hfnr.org.pl

B. Konieczna
e-mail: beata-konieczna@wp.pl

existing 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”). The results of the FRA research may therefore help to evaluate the improvements currently outlined in the European Commission’s proposal on data protection reform presented in January 2012.⁵

The FRA project will compare the relevant legislation and redress mechanisms concerning data protection in 16 Member States. Using both desk and social fieldwork research, the research aims to capture the experiences and views of the main actors concerned, such as—*inter alia*—individuals who suffered from data protection violations, legal practitioners dealing with the subject within their professional duties, and the data protection authority’s staff. The project’s final report will be published by the FRA in 2013.

This article will briefly summarize the most interesting preliminary findings of the study conducted in Poland.⁶ It will present both the general characteristics of the Polish study as well as certain phenomena specifically related to this particular national research. It will also discuss the most interesting views and experiences voiced by respondents participating in the project, which were used to identify common problems with regard to data protection provisions.

The general conclusion from the research is that the effectiveness of redress mechanisms in Poland is quite low. The article will attempt to identify the most serious barriers to efficient redress mechanisms as well as to recommend remedies. Hopefully, the conclusions drawn from the research may have a universal interest and provide some insight into what measures may be needed to improve the use of and access to redress for other countries facing similar encumbrances and in the context of the planned EU data protection reform.

2.2 Redress Mechanisms in Poland—Overview

The right to privacy and the principle of personal data protection were introduced to the Polish legal system in article 47⁷ and article 51⁸ of the country’s Constitution of 2 April 1997.⁹ These constitutional standards were further elaborated in the Personal

⁵ European Commission (2012).

⁶ The fieldwork was conducted between January and August 2012 by the Helsinki Foundation for Human Rights based in Warsaw which is FRA’s “National Focal Point” in Poland.

⁷ Article 47 of the Constitution: “Everyone shall have the right to legal protection of his private life and family life, of his honour and good reputation and to make decisions about his personal life”.

⁸ Article 51 of the Constitution: “1. No one may be obliged, except on the basis of statute, to disclose information concerning his person. 2. Public authorities shall not acquire, collect or make accessible information on citizens other than that which is necessary in a democratic state ruled by law. 3. Everyone shall have a right of access to official documents and data collections concerning him. Limitations upon such rights may be established by statute. 4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute. 5. Principles and procedures for collection of and access to information shall be specified by statute”.

⁹ The Constitution of the Republic of Poland (1997).

Data Protection Act of 29 August 1997.¹⁰ The provisions of the Personal Data Protection Act also implement the Data Protection Directive into the Polish legal system. The concept of personal data protection entitles any person whose rights have been infringed to request a review of the legality of the processing of their data. Under Polish law, there are three procedures for seeking redress in the field of personal data protection: administrative, civil and criminal. The choice of the procedure depends on the particular circumstances of the case. At some instances all these remedies can be applied simultaneously.

2.2.1 *Administrative Procedure*

The Code of Administrative Procedure¹¹ in principle is the legal basis for the proceedings conducted by the Inspector General for the Protection of Personal Data (“IGPPD”) pursuant to the Personal Data Protection Act. The IGPPD is an independent, central body of state administration appointed and dismissed by the Sejm of the Republic of Poland (lower chamber of the Parliament) upon the approval of the Senate (upper chamber of the Parliament). The general tasks of the IGPPD encompass the supervision of the compliance of data processing with the provisions of the Personal Data Protection Act. The proceedings initiated by the IGPPD may be launched upon receiving a complaint, or *ex-officio*. The proceedings should be concluded with an administrative decision determining whether a data protection violation has occurred.

In case of any breach of the provisions on personal data protection, the IGPPD shall, by its administrative decision, restore the proper legal state. In particular, the IGPPD may order to remedy the negligence, to complete, update, correct, disclose, or not to disclose personal data, to apply additional measures protecting the collected personal data or to erase personal data.¹² Parties that are not satisfied with the administrative decision have 14 days, from the date of delivery, to apply to the IGPPD for the re-examination of their case.¹³ Further on, if the IGPPD determines to uphold the original challenged decision, the party has 30 days to file a complaint with the Provincial Administrative Court in Warsaw. A judgment delivered by a first-instance court may be challenged by lodging a cassation complaint with the Supreme Administrative Court. The complaint must be made within 30 days from the day a copy of the reasoned decision is served on the parties. The proceedings before the administrative courts are governed by the Administrative Courts Procedure.¹⁴

¹⁰ Personal Data Protection Act (1997).

¹¹ The Code of Administrative Procedure (1960).

¹² Article 18 of the Personal Data Protection Act.

¹³ Article 21 (1) of the Personal Data Protection Act: “A party may submit a motion to have their case reconsidered with the Inspector General”.

¹⁴ The Administrative Courts Procedure Act (2002).

The IGPPD cannot impose financial penalties for data violations. In order to increase its effectiveness, the IGPPD was afforded a power to enforce duties imposed by virtue of its decisions. This includes the authority to impose a coercive fine on entities that fail to perform administrative decisions issued by the IGPPD.¹⁵ The maximum fine amounts to PLN 10,000 złotych (around 2,500 €) for natural persons and PLN 50,000 złotych (around 12,500 €) for legal persons. In addition, the IGPPD may intervene with various authorities and entities in order to ensure efficient protection of personal data. It may also request competent authorities to issue or to amend legal acts in cases relating to personal data protection. Importantly, the entity shall give an answer in writing to any address or request made by the IGPPD within 30 days following its receipt.¹⁶

2.2.2 *Criminal Procedure*

Chapter 8 of the Personal Data Protection Act contains provisions on the criminal liability for offences defined in articles 49–54a of the Act. They include, *inter alia*, offences such as: disclosure or providing access to data to unauthorized persons, processing personal data in a data filing system where such processing is forbidden, violation of the obligation to protect data against unauthorized access, damage or destruction, failure to provide data subjects with obligatory information about their rights with regard to data processing, or hindering the performance of inspection activities performed by the IGPPD. The offences are prosecuted by the law enforcement bodies in accordance with the general procedural rules laid down in the Code of Criminal Procedure.¹⁷ Under the applicable criminal provisions laid down in the Personal Data Protection Act, the possible criminal sanctions, depending on particular offences are a fine and restriction or deprivation of liberty. The term of imprisonment ranges from less than a year, if the infringing party acted inadvertently, up to 3 years, if the offence concerns sensitive data.

2.2.3 *Civil Procedure*

Unauthorised processing of personal data may also be a cause of action in a case involving an infringement of personal rights, which include protection of privacy and personal data. Pursuant to article 23 of the Civil Code¹⁸, personal rights (such as health, freedom, dignity, freedom of conscience, surname, pseudonym, or image) are protected in civil law, notwithstanding the protection granted by virtue of other

¹⁵ Article 12 (3) of the Personal Data Protection Act.

¹⁶ Article 19a of the Personal Data Protection Act.

¹⁷ The Code of Criminal Procedure (1997).

¹⁸ The Civil Code (1964).

legal enactments. Under article 24 of the Civil Code, the legislator allowed for several kinds of remedies in the event of personal rights violation. The claimant may seek the remedy of the results of the infringement through—for example—a publication of apologies. They may also seek compensation in the case when a moral and pecuniary damage occurred (they may also ask the defendant to make a donation for a charitable or community purpose). Civil proceedings are commenced with a plea filed with the court by the claimant (the data subject) against the defendant (person responsible for the data protection violation). Against the judgment of the first instance court, the parties can lodge an appeal with the second instance court and then also a cassation appeal (last resort appeal) with the Supreme Court. In the civil proceedings concerning the infringement of personal rights, the claimant's position is stronger as they may benefit from the "presumption of unlawfulness" of the defendant's action. This means that the claimant needs to only prove that his personal rights have been infringed, putting forward evidence confirming the infringement. It is the defendant, on the other hand, who must satisfy the court that his or her actions have been taken legally (e.g. there existed a legal basis for the processing of a claimant's personal data).

2.3 Characteristics and Methodology of the Research Study in Poland

The fieldwork research on the redress mechanisms in the field of data protection took place between January and August 2012 and comprised 36 one-to-one interviews with three groups of respondents: 15 individuals who have sought redress ("complainants"), 15 individuals who have experienced data protection violations but have not sought redress on that account ("non-complainants"), and judges and prosecutors conducting cases which involve data protection violations. Three focus group discussions were also conducted as part of the research. The targeted groups included the IGPPD's staff, members of non-governmental organisations working in the field of data protection, and advocates and legal counsellors specialising in data protection law.

In the group of complainants, out of 15 respondents—10 initiated criminal proceedings, 7 commenced administrative proceedings and 4 brought civil actions (some of the respondents initiated more than one procedure at the same time). In the non-complainants group, the respondents most frequently stated that they had considered taking administrative actions (9 out of 15 respondents). The second most popular measure was alternative dispute resolution procedures, such as settlements (indicated by 8 respondents). Only 3 respondents considered bringing their case before a criminal or civil court. Respondents were allowed to list more than one potential redress procedure.

Respondents pointed out a series of events in which they had faced personal data violations. The most common situations concerned unlawful personal data processing by governmental bodies as well as private financial institutions and marketing

companies. Personal data violations very often included disclosing data for commercial purposes, resulting *inter alia* in unwanted telemarketing calls to the respondents' private phone numbers. Many respondents also complained about breaches involving the use of the Internet, such as their personal data being posted on-line or unsolicited information being sent to their e-mail addresses. Moreover, there were some violations mentioned which were committed by employers from both the private and public sector with regard to the processing of a broader range of employees' personal data (including for example biometric data) than prescribed in Polish employment law. There was also one reported case in which personal data were unlawfully collected and processed by one of the intelligence agencies and one case in which there was an excessive use of CCTV cameras.

The general starting point for a reflection on redress mechanisms in most respondents' cases was a subjective sense of harm and a feeling that the boundaries of an acceptable level of interference with their privacy had been crossed. The greater the sense of infringement, the more willing they were to seek redress. One of the respondents pointed to the "aggregation effect" of data violation. This means that a decision to take specific legal steps is taken on the basis of a subjectively understood aggregate of data violations. One of the main motivating factors for the respondents to seek redress was a desire to counteract the abuse of public power, publicize the problem and draw attention to the violating of personal data protection law by the state and local authorities; another important motivation was a desire to obtain compensation for a data protection violation. The compensations did not have to be financial, but could be limited to an obligation to publish apologies, for example. Finally, the respondents claimed that what drove them to take legal measures was very often a personal aversion towards the breaching party (for example an ex-employer) and the desire to "punish" them by imposing some kind of penalty on them for their misconduct.

2.4 Barrier No. 1: A Lack of Education on and Low Awareness of Data Protection

The first barrier to effective redress mechanisms identified by the results of the study is the low awareness and lack of education on data protection issues among data subjects. The main reason for not seeking redress in the case of non-complainants was that very often they were unable to define if they actually had faced a data protection violation. They could not always link the negative emotions they experienced with regard to a particular situation with the infringement of their right to privacy. They were unable to assess if the harm they suffered was "serious enough" in order to legitimately claim their rights or whether it fell within the scope of the data protection law. Some respondents were also not aware of the existence and the characteristics of a personal data protection body (this applies not only to the individuals suffering from data protection violations, but sometimes even the members of the judicial community).

Regarding the complainants who could recognize data protection violations, the vast majority did not have sufficient information about the redress mechanisms that could be applied in their cases. They were usually not aware of different redress mechanisms at their disposal (civil, penal or administrative) and what outcome they could expect from particular procedures. The lack of knowledge in this respect very often led to the very low level of satisfaction with regards to the results of the proceedings they had decided to initiate. Even if the outcome turned out to be positive for the respondents, it did not meet their expectations and eventually caused disappointment.

For example, for those complainants who sought redress intending to obtain compensation or “punish” the data controller responsible for the data protection violation, the administrative procedure before the data protection authority was unsatisfactory. For many complainants application to the IGPPD seemed the most “natural choice” as they perceived it as the most well-qualified and specialized body in the area of data protection issues. At the same time, there is a low public awareness with regard to the IGPPD’s actual competences, which are more limited than many respondents expected. Most of the respondents initiating administrative procedure before the IGPPD were not aware that it is not competent to award compensation for moral damage (which is a competence reserved by the civil court). Furthermore the IGPPD is not intended and authorized to impose criminal penalties on individuals liable for unlawful data processing (which is a competence reserved by the criminal court). With regard to criminal proceedings, if the IGPPD decides that an action or omission of a person responsible for violation contains all requisite elements of the offence laid down in the Personal Data Protection Act, it can only report the offence to the law enforcement body, which may then take further actions. What is more, the IGPPD’s competences are even more limited if in the meantime the data controller remedies the violation. The IGPPD may intervene only with regard to existing violations.

That is why in many respondents’ opinions the administrative proceedings conducted by the IGPPD followed by the judicial administrative proceedings carried out by the administrative courts fail to provide complete protection, as they do not have the effective compensatory or punitive function. The vast majority of respondents were not aware these results could be achieved through civil or criminal proceedings before civil or criminal courts and not by the administrative procedure.

The low level of public awareness regarding data protection issues and redress mechanisms results from a lack of education and lack of easy access to information. The main and primary source of knowledge for the respondents was the Internet. However, many of them stated that the online sources are fragmented, unclear and not sufficiently accessible. According to the respondents, there is no website which would offer a comprehensive guide to the available redress mechanisms, a list of the stages of the proceedings, and the rights and obligations of individuals pursuing legal redress procedures. For example the respondents noted that the website of the IGPPD does not entirely serve this purpose, even though it contains an on-line educational platform. They noted that the way it is written is too formal and in language which is not user-friendly; moreover, it is incorrectly positioned on the web in search engine results and therefore difficult to access. On the other hand it was not very

common for the respondents to obtain knowledge on the area of data protection through professional legal assistance, which was believed to be excessively costly.

To sum up, despite the existence of three different kinds of procedures, which in some instances can be applied simultaneously, their existence does not improve the effectiveness of the redress mechanisms. This is because people seeking redress for data protection violations are not aware of the existence of these measures; they do not distinguish them, they do not always understand their characteristics or they do not have sufficient knowledge about how they should be applied.

2.5 Barrier No. 2: The Insufficient Enforceability of Data Protection Law

The second barrier weakening the effectiveness of the redress mechanisms in Poland mentioned by most of the respondents was the insufficient enforceability of data protection law. This applies especially to the criminal procedure that was evaluated as the least effective by both the complainants and focus group interview participants such as the IGPPD's staff and judges.

The complainants who had tried to initiate the criminal proceedings reported that they had had the impression that criminal judges and prosecutors were not familiar with personal data law, tended to be unwilling to investigate such cases, and underestimated its serious character. According to the complainants and the IGPPD's staff, it is mainly the prosecutors who are not prepared to apply data protection provisions. The study revealed that a low level of expertise in the field of personal data protection among law enforcement authorities is the result of the absence of any extended coverage of this area during legal vocational courses or subsequent training. These educational shortcomings may generate a negative attitude towards prosecuting data protection cases. That is why most respondents' cases concerning data protection violations were discontinued by prosecutors as "negligible social harm"; only in a few cases did the prosecution eventually bring the indictment to the court. This view was also confirmed by the annual report on the IGPPD's activities for 2011.¹⁹ The report states that the analysis of the pre-trial proceedings conducted by the prosecution leads to a conclusion that a very small number of cases end up in court. According to the report, there were only two sentencing judgments by the criminal courts in 2011 resulting from the IGPPD's notification of crimes in previous years (in 2010 the IGPPD made 23 notifications, in 2009—27, in 2008—31). The prosecution does not provide data on the general number of crime notifications concerning data protection violations.²⁰

In the prosecutors' opinion there is a whole range of factors contributing to the negative perception of the activity of the prosecution service and its preparation for handling data protection cases. The prosecutors claimed that criminal provisions

¹⁹ IGPPD (2012, p. 243–244).

²⁰ The response of the Prosecutor General to the Helsinki Foundation for Human Rights (2012).

contained in the Data Protection Act are poorly drafted in the first place. In the majority of cases they cannot be applied because the reported crimes do not contain all the requisite elements of an offence laid down in the law. Moreover, prosecutors consider data protection provisions to be “detached from real life”. The prosecutors also complained about the lack of professional training on data protection issues and specifically noted the need to organize training courses on this topic to enhance the competence of the prosecution service. They also stated that they consider the criminal liability for data protection violations extensively severe, disproportional and therefore expressed the view that these kinds of cases should be handled under administrative and not criminal law. Especially due to the limited resources at the prosecution office forcing them to focus on “more serious” crimes. Some of the prosecutors (and other respondents) even suggested that the criminal provisions should be abolished from the Personal Data Protection Act.

According to the members of the focus group interviews, the most effective legal remedy to data protection violations is the civil procedure. That is because it may bring a desirable and satisfactory outcome to the claimant (financial compensation, apologies, etc). Moreover in cases involving the protection of personal data (falling under the heading of personal rights), the claimants have a much better position at the trial as they benefit from the “presumption of the unlawfulness” of the infringement. But the most effective civil measure is at the same time the least popular one. The respondents’ top two choices in selecting a redress mechanism were the criminal and administrative procedures, whereas the civil procedure was considered an alternative that might be used if the first two mechanisms fail. Only 4 out of 15 complainants took advantage of civil law instruments. The respondents perceived the civil procedure as the most expensive, complex, and long-lasting process (which is not always true) and were not aware of its positive aspects. They also perceived the civil procedure as the most engaging for the party and they were anxious that they would be “left on their own” during the trial (especially if they could not afford a professional legal aid). For the criminal or administrative procedure, the respondents believed they would be offered “support” from the IGPPD or the prosecution during the proceedings.

2.6 Barrier No. 3: The Data Protection Law—its Complexity and Limited Scope

The third barrier which lowers the effectiveness of the redress mechanisms that was identified by the respondents is the complexity of the data protection law, namely: the formalism and lack of transparency of the procedures as well as its extensive duration (and the fact that it is very hard to assess the length of the proceedings). The language of the Personal Data Protection Act itself was also described by most of the individual respondents as difficult and discouraging.

The problem of the complexity of the procedures was very well reflected by the information provided by the representative of the IGPPD’s staff who claimed that around 80 % of the complaints submitted to the data protection authority for the

first time contain formal defects and they have to be returned to the complainants in order to be remedied. This applies not only to the complaints filed by individuals, but also by professional attorneys. Only after the formal defects had been remedied, could the complaint be re-submitted and further proceeded with, which significantly prolongs the procedure. Most of the respondents also noted that they were unable to use the Internet document filing system on the IGPPD's website because it seemed too complicated. Furthermore the respondents questioned the mechanism of the IGPPD's reconsideration of its own decisions, which is obligatory before filing the complaint to the administrative court. Many respondents claimed it was not effective and a time-consuming legal remedy which unnecessarily extends the procedure.²¹

Another problematic issue indicated by the respondents were the numerous limitations to the inspection powers of the IGPPD under the Polish Data Protection Act. Examples of these jurisdictional gaps that were specifically reported during the study were the IGPPD's inability to verify whether an apostate's records have been deleted from parish records and the lack of a mechanism for establishing the scope of data processed by the Central Anti-corruption Bureau ("CBA", one of the Polish intelligence agencies).

Over 30 individuals who made an act of apostasy²² from the Catholic Church answered the call to participate in the research. A member of this group was interviewed as part of the complainants' group. He described situations where parish priests refused to delete the apostates' personal data from parish records. At the same time he claimed that the apostates were unable to complain to the IGPPD whose jurisdiction is excluded with regard to processing data for the purposes of a church or religious association.²³ Therefore under the current Polish Data Protection Law the IGPPD is not competent to issue an administrative decision obliging the church to remove or correct the personal data processed within its books. Some of the apostates formed an active group aimed at effecting change in the applicable provisions governing the issue of leaving the Catholic Church. One of the group's initiatives was the creation of a website which contains a comprehensive, step-by-step guide to the

²¹ Pursuant to the Code of the Administrative Procedure and the Administrative Courts Procedure the IGPPD must issue an administrative decision within 30 days after receiving a complaint. In the course of 14 days after the date when the original decision is served on the party, the party may ask for reconsideration of the case by the IGPPD. Only after the second decision is issued and served on the party, the party has 30 days for challenging the decision before a Provincial Administrative Court.

²² Apostasy is currently understood as a conscious, voluntary and public defection from the Church. On 29 September 2008 the Polish Episcopal Conference laid down a procedure for persons wanting to make an act of apostasy in one of the Polish dioceses. Under this procedure an aspiring apostate shall deliver a statement drafted personally to the parish priest in his or her place of residence in the presence of two adult witnesses. The priest has an obligation to confirm the receipt of such a statement with his handwritten signature and a parish seal and to send the same to the diocesan curia which further instructs the priest to make an appropriate entry in the parish register of baptism. The note that a person has left the Church should be permanently entered on the margin of this person's certificate of baptism kept in the register of baptism. Under the ecclesiastical law an entry of baptism must not be deleted from the register of baptism.

²³ Article 43 (2) of the Personal Data Protection Act.

Reloading Data Protection

Multidisciplinary Insights and Contemporary Challenges

Gutwirth, S.; Leenes, R.; de Hert, P. (Eds.)

2014, XV, 369 p. 13 illus., 5 illus. in color., Hardcover

ISBN: 978-94-007-7539-8