The synthesis of the Annual Report on the activities of the President of the Personal Data Protection Office in 2023

Report on what the President of the Personal Data Protection Office did in 2023 and the conclusions, resulting from the state of compliance with personal data protection legislation, drawn for the future.

Introduction

Personal data are one of the most valuable assets of the modern world. It is thanks to them that the data-driven economy is developing and that countries are creating better policies, because they are tailored to the needs of citizens. However, personal data can be used as a dangerous weapon and a tool for manipulation. Therefore, they should be treated with care and processed with the least possible risk for the data subjects.

The authority that deals with the protection of personal data and the right to privacy in Poland is the President of the Personal Data Protection Office. Its task is to check how Polish and European data protection regulations are complied with. It issues guidelines, interprets the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, also known as the General Data Protection Regulation) and handles complaints. It can impose fines, as well as indicate what needs to be changed in the organisation so that personal data are better protected, with less risk for the data subjects.

The President of the Personal Data Protection Office also carries out educational activities on personal data protection and the right to privacy. This document, which is a synthesis of the authority's Activity Report 2023, and which, pursuant to Article 59 of the GDPR, the President of the Personal Data Protection Office presents annually to the Sejm of the Republic of Poland (lower chamber of the Polish Parliament) - is part of this activity.

The authority’s Annual Report 2023 is available at: https://uodo.gov.pl/pl/p/o-nas. It relates to the period when the function of the President of the Office was fulfilled by Jan Nowak. Since January 2024, the President of the Personal Data Protection Office has been Mirosław Wróblewski, elected to this position by the Sejm with the consent of the Senate (upper chamber of the Polish Parliament) on 17 January 2024.

IT IS WORTH KNOWING:

Everyone shall have the right to the protection of personal data concerning him or her. This right is guaranteed by the Constitution of the Republic of Poland (Article 51 in conjunction with Article 47), the Charter of Fundamental Rights of the European Union (Article 8), and the Treaty on the Functioning of the European Union (Article 16).

Detailed provisions for the implementation of this right are mainly introduced by the GDPR, specifying the principles of data processing, the related obligations of controllers and the rights of data subjects

The GDPR is a regulation jointly developed and adopted by all Member States of the European Union. It is applicable throughout the Union.

Complaint to the President of the Personal Data Protection Office about unlawful personal data processing (Art. 50 of the Act on the protection of personal data processed in connection with preventing and combating crime).

1. A person whose personal data are processed unlawfully has the right to lodge a complaint with the President of the Office within 30 days of becoming aware of the breach or receiving information from the controller
2. The President of the Office shall provide the person who has lodged the complaint with legal assistance on such person's request pending the examination of the complaint by the President of the Office.
3. A complaint can be lodged using the form posted in the Public Information Bulletin on the homepage of the President of the Office, in writing, by fax, electronically or using the electronic platform of public administration services - ePUAP.
4. The President of the Office shall inform the person who has lodged the complaint of the progress of its investigation, the manner in which it was handled and the possibility of lodging a complaint with the administrative court. The provisions of Articles 225 (the obligation to prevent the restriction of the right to lodge complaints and requests), 231 (exclusion of the application of the act_231) and Articles 237-239 of the Code of Administrative Procedure shall apply *mutatis mutandis* to the handling of complaints.
5. The President of the Office shall not provide the person lodging the complaint with information which may indicate that personal data are processed by the competent authorities in the situations referred to in Article 26(1) (inadmissibility of the transfer of information and disclosure of personal data).
6. The right to notifying a breach of the processing of personal data shall also apply to persons other than those mentioned in subparagraph 1 if they become aware of such a breach in a reliable manner. Article 225 of the Code of Administrative Procedure shall apply *mutatis mutandis* to the processing of applications (the obligation to prevent the restriction of the right to lodge complaints and requests).
7. The data of the notifying party referred to in subparagraph 6 shall be kept confidential by the President of the Office upon a justified request of that party.

ACTIVITIES OF THE PRESIDENT OF THE PERSONAL DATA PROTECTION OFFICE IN 2023

Answers to citizens' questions

In case of any problems or concerns regarding the application of personal data protection legislation, one can call the Personal Data Protection Office (tel. no. 606-950-000).

Each day, the infoline staff answered dozens of calls. There were over 14,000 such calls in 2023, which is an average of 57 calls per day. Both natural persons and representatives of legal and public entities called.

The most frequent questions addressed to the Office's infoline:

- **video surveillance** (neighbourhood, private, housing communities, in educational institutions, in workplaces, in pharmacies, in hospitals, in car parks);
- **processing of personal data by housing cooperatives and housing communities**;
- **processing of personal data by employers** (e.g. retention of employee CVs, health data, drug testing and employee sobriety testing vs. GDPR, remote working application vs. data of a disabled family member, employee monitoring);
- **law infringements in the education sector** (recording of a pupil by a teacher, taking photographs of a pupil, disclosure of special categories of data);
- **unsolicited telemarketing;**
- **requesting scans of identity documents by online sales platforms** in order to unblock funds received from sales (e.g. Allegro, Vinted, Olx);
- **passenger verification procedures** applied by airlines.

Complaints by citizens

A person who believes that his/her personal data are being processed unlawfully has the right to lodge a complaint with the President of the Office. Complaints addressed to the President of the Personal Data Protection Office concern various aspects of everyday life - from issues concerning data processing by a neighbour (e.g. video surveillance), to complaints against employers and government administration institutions

In 2023, the Personal Data Protection Office received **6962 complaints from citizens** (33 fewer complaints than in the previous year). Cases handled on the basis of complaints at the Office are increasingly complex and multifaceted and increasingly involve issues related to new technologies.

The most dramatic complaints in 2023 concerned situations of disclosure of personal data that could lead to suicide (DOL.023.173.2023, DOL.051.6.2023.).

The first of these cases concerned a minor whose personal data were disclosed in a media release concerning the conviction of an adult for a paedophile act. The information was disclosed to attack the child's mother, who is a public figure. The information provided made it possible to identify the child who had been harmed. Shortly after this information was revealed, the young person committed suicide.

The second case involved the disclosure on social media of a person's details in the context of a claim that the person had allegedly committed an indecent act in a public place and was alleged to have committed an act of a paedophilic nature. The scope of the data disclosed included information about the fact that the person was serving as a priest, the name of the congregation and an image.

In both cases, the then President of the Personal Data Protection Office refused to handle the cases, deciding that there were no legal grounds to initiate proceedings.

The current President of the Personal Data Protection Office has taken steps to clarify the circumstances under which these individuals' personal data were made public. Proceedings in these cases are ongoing and will be presented in the authority's 2024 Activity Report.

Everyday matters

The President of the Personal Data Protection Office investigates lodged complaints, may issue a reprimand, issue an injunction, and in special situations - impose a fine.

Many of the complaints that the President of the Personal Data Protection Office handles concern issues related to the operation of housing communities and housing cooperatives.

Here are examples of such complaints:

Disclosing personal data of a person who challenged a resolution of the housing community to other members of a community. In an administrative decision, the President of the Personal Data Protection Office found that the disclosure of those data was not necessary to inform the community about a legal dispute with one of its members. The case ended with a reprimand.

Right of access vs. video surveillance. The housing community did not want to give the resident the CCTV footage that showed his or her image. It explained that there were other people on the recordings. Meanwhile, access to one's data is a right guaranteed by the GDPR. This case also ended with a reprimand and an order to release the footage.

Disclosure of data of an indebted housing community's member in the manager's email to the community. The President of the Personal Data Protection Office pointed out that the assertion of a claim by the community does not require all members to know the debtor's data. It admonished the community for the breach.

Examples of 2023 cases in which the President of the Personal Data Protection Office applied fines:

- A housing cooperative in conflict with one of its members, filed a notice of suspicion that the person had committed a crime. A copy of the notice, with the personal data of the cooperative's member, was provided by the cooperative to journalists. These data were obtained by a person associated with the media circles, who did not request these data at all. However, the cooperative did not report the breach to the Personal Data Protection Office or communicate it to the person whose data was included in the document. In this case, the President of the Personal Data Protection Office imposed a fine on the cooperative (data controller) and ordered it to communicate the breach to the person whose data had been disclosed.
- The housing community's manager (processor) had documents stolen, including a deed. The housing community, which is the controller of these data, did not notify the breach to the President of the Personal Data Protection Office (the latter received an anonymous notification on the matter) and did not communicate it to the persons whose data were in the deed. Moreover, in the course of the

proceedings, it turned out that the processing of the data of the members of this community was entrusted to a property management company without a written contract and without verifying whether this entity provides sufficient guarantees for the implementation of appropriate security measures. The President of the Personal Data Protection Office imposed a fine on the community.

NOTE! If the penalised person does not agree with the decision of the President of the Personal Data Protection Office (on a reprimand or fine), he or she may appeal against the administrative decision to the Voivodeship Administrative Court in Warsaw. The court either upholds the President's decision or revokes it.

Example:

The Voivodeship Administrative Court in Warsaw (II SA/Wa 763/22) upheld the decision of the President of the Personal Data Protection Office in 2023 that the housing community should remove the complainant's personal data (his or her image) from the video surveillance recordings of the waste disposal facilities and stop making such recordings. The court shared the position of the supervisory authority, finding that the community had not demonstrated that the prerequisites allowing such processing of personal data had occurred. Balancing the interests of the data subject and the controller is mandatory. The fundamental rights and freedoms, on the one hand, and the legitimate interests of the controller, on the other hand, must be assessed and balanced with care.

The Voivodeship Administrative Court in Warsaw (II SA/Wa 1340/22) raised the issue of private monitoring and the related information obligation under Article 13 of the GDPR. The President of the Personal Data Protection Office found that the scope of the video surveillance belonging to the neighbours complained against extends beyond their property to include common space (co-ownership). The neighbours' indicated need to ensure their own safety and that of their children is a justification for monitoring limited to the area of the property of which they are the sole owners. The President of the Personal Data Protection Office therefore ordered the monitoring coverage to be limited and issued a reprimand, which the Voivodeship Administrative Court upheld.

Notification of breaches by controllers themselves

Under the GDPR, a data controller is obliged to notify to the President of the Personal Data Protection Office an incident that has resulted in a data breach and is likely to have a detrimental effect on data subjects (e.g. so-called identity theft). In doing so, the controller should independently analyse how the data breach occurred at its company and present what measures it has implemented or intends to implement in order to avoid a similar situation in the future. The Personal Data Protection Office shall analyse such a breach and, if necessary, take such action as it deems appropriate.

In 2023, the Personal Data Protection Office received **14,069 personal data breach notifications.**

The President of the Personal Data Protection Office noted in 2023 that controllers are doing this more and more frequently, and when submitting breach forms again, they are able to accurately assess whether there is a high risk to the rights or freedoms of natural persons and determine after analysis whether to communicate the breach to data subjects. At the same time, Data Protection Officers (DPOs) were increasingly able to identify security measures that should be implemented to avoid similar incidents.

What were the subjects of notifications? Examples:

- **incorrectly addressed correspondence**. A very frequently notified breach is the sharing of personal data with the wrong addressees in mass mailings sent without hiding the email addresses of others (Bcc);
- **making data available to the wrong person**, e.g. by issuing documents such as certificates or tax declarations to persons who are not entitled to receive them or by incorrectly sending correspondence with data;
- **incorrect anonymisation of data or inadvertent publication**, e.g. on a website or in response to a request for access to public information;
- **unauthorised access to databases**. Such breaches were most often caused by software bugs revealing themselves after a programme update, a lack of regular internal security testing, and irregularities at the authorisation stage in IT systems;
- **paper documentation being lost, stolen or left in an unsecured location.** Breaches of this kind were one-off incidents and were the consequence of staff carelessness;
- **loss or theft of a data carrier (laptop or unencrypted memory stick);**
- **a hacking attack using malware** that interferes with the confidentiality, integrity or availability of personal data;
- **breaches caused by application errors** allowing unauthorised access to resources, through access to the identifier of the indicated resource (IDOR vulnerabilities).

The President of the Personal Data Protection Office, in the case of complaints and breach notifications, has the right to call on the controller to provide additional information or to indicate the actions necessary on the controller's side. In 2023, these actions generally proved to be effective: controllers took steps to ensure effective protection of personal data.

Decisions of the President of the Personal Data Protection Office

It is crucial for the protection of the data subject that she or he can lodge a complaint with the supervisory authority when she or he considers that the processing of her or his data breaches the provisions of the GDPR. The role of the President of the Personal Data Protection Office is to ensure that the complaint is handled in an independent, appropriate and compliant manner. Handling complaints from data subjects is a task to which the President of the Personal Data Protection Office attaches particular importance.

Analysing complaints and data breach notifications in 2023 (including complaints and notifications received in previous years), the President of the Personal Data Protection Office issued **1750 decisions**. The number of cases concluded with an administrative decision is at a constant level. Decisions of the supervisory authority were appealed to the Voivodeship Administrative Court in Warsaw in 223 cases (for comparison: 177 decisions were appealed in 2022). In the majority of cases, the administrative courts shared the positions taken by the

President of the Personal Data Protection Office in complaint cases. In 2023, the appeals against judgments issued by the Voivodeship Administrative Court in Warsaw to the Supreme Administrative Court increased - from 55 in 2022 to 66 in 2023.

When the investigation, related to a notified data breach, does not lead the President of the Personal Data Protection Office to satisfactory results, it initiates administrative proceedings. In 2023 the President of the Personal Data Protection Office initiated 24 such proceedings and completed 36 proceedings that had also started in previous years, 17 of which ended with reprimands and 19 of which also ended with fines. Seven decisions on fines were appealed to the Voivodeship Administrative Court in Warsaw. The Court upheld 4 and annulled 2 decisions. The rest of the cases are pending.

Inspections of the President of the Personal Data Protection Office

The President of the Personal Data Protection Office carried out inspection activities with regard to compliance with the provisions on personal data protection in **33 entities**. These included.

- **a health industry entity** where a large amount of personal data leaked as a result of a hacking attack and security breach;
- **an insurance industry entity** - the inspection showed that insurance intermediaries (natural persons performing agency activities) had access to a customer database containing data such as name, address, personal identification number (PESEL number), e-mail address and telephone number;
- **a medical facility** - the inspection concerned the processing of personal data by technical means allowing video or audio recording;
- **a courier company** - the inspection covered the company's processing of personal data in connection with the provision of a courier delivery service, in particular adequate protection of delivered good against loss and destruction.

The President of the Personal Data Protection Office paid particular attention to mobile and web applications.

The inspection of the President of the Personal Data Protection Office covered 15 entities using mobile applications (industries: medical, banking, trading, catering, tourism, transport, as well as public administration).

In 2023, in accordance with the sectoral inspection plan, the President of the Personal Data Protection Office also inspected five entities using Internet (web) applications. These entities operated in the insurance, trading, bookmaking and hosting industries.

The inspections relating in particular to how personal data processed with the use of web applications are secured and disclosed are still ongoing and will continue into 2024.

Requests of the President of the Personal Data Protection Office

In 2023, the President of the DPA issued 5 specific **requests** to public administration authorities and private entities operating in various sectors, of which 2 concerned legislative issues, while the impetus for 3 requests was signals received from Data Protection Officers. This compares to 16 requests in the 2022 reporting year.

Potential of the Personal Data Protection Office

At the end of 2023, the Personal Data Protection Office had 267 employees. The Office's budget amounted to PLN 45 million 367 thousand in 2023.

Art. 35 of the GDPR. A revolution in thinking. Estimating risks rather than tracking culprits.

Analysis of breach notifications, complaints and inspection results shows that data protection related errors can be accidental, e.g. as a result of an unfortunate coincidence. But they can also be a symptom of systemic problems - inadequate attention paid to the protection of personal data, poor knowledge of those running organisations or a lack of security procedures. And, above all, the fact that we still do not think in terms of **risk analysis**.

It is easier for us to look for someone to blame when a problem arises than to assess the risks in advance and, on the basis of this analysis, take appropriate remedial measures before a problem occurs.

The principle of a risk-based approach is an important forward-looking concept. It forms the core of the GDRP. It implies that no strictly defined security measures and procedures are indicated to controllers and processors. They themselves must carry out a detailed analysis of the data processing operation and assess the risks on this basis, depending on the nature, scope, context and purposes of the processing. They assess the risks to the rights and freedoms of the data subjects as well as the risks to the interests of the controller.

Thus, for example, different protection measures should be taken in the case of the processing of data by a shop that sells online and by a shop that sells only on the premises which does not process its customers' data with the use of ICT systems using the Internet.

When talking about the risk to the rights and freedoms of individuals under the GDPR, it is necessary to take into account:

1) the likelihood of a particular event occurring
2) the severity of that event, i.e. the magnitude of the damage that the event may cause.

It is about this risk analysis: what it looks like and how it was updated, that the President of the Personal Data Protection Office asks when conducting its proceedings.

The way of conducting risk analysis is described in Art. 35 of the GDPR.

Processing of personal data - A business issue

The use of modern data-driven technology is a great way for small and medium-sized businesses to grow. The problem is that technology not only streamlines old procedures and allows tasks to be completed faster. It also poses new challenges for entrepreneurs. Data collected digitally and processed on an ever-increasing scale require risk analysis and

constant attention. It is not enough to outsource this task to an IT team or a Data Protection Officer. Data protection thinking must be embedded throughout the organisation.

Mobile applications

Mobile apps are such a new convenience for businesses.

By the beginning of 2022, there were more than 6 million of them worldwide. Almost every one of them collected information about its users. Many mobile apps collect data that identify a specific user - these are generally those apps that require the creation of an account and the provision of personal data necessary to use their functionality. Some mobile apps collect data that on the surface may appear to be anonymous, but from a legal point of view (and in conjunction with other data processed) may 'become' personal data. Such data are also subject to protection.

The development of mobile apps is the best time to ensure that this product is compliant with data protection principles and therefore developers should consider data protection requirements from the design stage.

The sectoral inspection carried out by the President of the Personal Data Protection Office in 2023 covered in particular:

1) security elements to protect personal data processed in mobile applications and in related IT systems,

2) mechanisms for creating and verifying backups,

3) principles of using anti-virus, anti-spam and other systems supporting the protection of mobile applications and IT systems,

4) methods of logging and controlling events in IT systems,

5) the way of granting access to the processed personal data (with particular emphasis on the mechanisms ensuring confidentiality, integrity, availability of data),

6) control of methods and scope of informing users of mobile applications about the nature of access of these applications to functionalities embedded in mobile devices.

What did it produce? The inspection showed that business is improving at dealing with mobile apps, although there are still issues to watch out for.

For example, an inspection at one **medical facility** showed that a user was entering his or her personal identification number (PESEL number) as a login to launch a mobile app. There were several thousand accounts. Thus, the process of logging into the app was large-scale processing of personal data. A properly conducted data protection impact assessment would have immediately identified the risks associated with establishing the personal identification number as a login.

An inspection at a **company operating an online food ordering platform and using a mobile app** found that excessive data were being collected from customers. The company was

requesting scans of ID cards or passports from customers, which is against the principle of data minimisation.

In general, it should be concluded that the inspected entities have implemented the required technical and organisational measures to ensure an adequate level of data security. They have prepared and implemented security policies, concerning passwords and cryptographic measures. They also continuously monitored the security of systems, used anti-spam and anti-virus systems, carried out periodic security tests, encrypted files and media, monitored the flow of data to and from media, and used two-factor authentication. Security systems (e.g. firewalls, detection and response systems) and systems ensuring accountability of operations performed on personal data were used to protect against attacks from the public network. Inspected entities attached great importance to the accessibility of their services to users.

The use of data processing intermediaries

Many entrepreneurs use online platforms. They may, for example, entrust customer data to marketing companies. The important point here is that they are still data controllers and have obligations because of this.

An example of the problems that arise from negligence and from failure to fulfil duties and end up in the intervention of the President of the Personal Data Protection Office is the case of a citizen who received text messages from a marketing company and demanded the removal of his or her data from the database - meanwhile, it was another company that was the controller of the data and entrusted them to a marketing campaign. It handed them over without the consent of the data subjects. It was not thinking in terms of data protection, but only - to improve its business. It ended with an explanation to the President of the Personal Data Protection Office and with a reprimand.

Routine in staff documents and in proceedings

This type of mistake could have gone unnoticed in the pre-digital era: a document containing one person's data was treated as a template for others. The template was on paper, so the data didn't circulate globally. Now, things are different. A person lodged a complaint with the Personal Data Protection Office, having discovered that his or her data from a legitimate fixed-term contract with a company were still being used as a template. These data were circulating online, including his or her name, address, salary, job position, and bank account number.

Other bad practices can also be identified, such as informing an entire team during a meeting about the detailed reasons for terminating an employee’s contract. In the digital age, such practices become a serious issue. This was the case with a citizen who filed a complaint with the Personal Data Protection Office, as a detailed description of the termination of her employment was shared in an email sent to all employees. The Labour Code does not give the employer grounds to disclose such information. Digital communication exacerbates the problem.

GPS in a company car

This is a new and popular form of controlling whether employer-owned equipment is being used for its intended purpose and not, for example, for an employee's private use. The point is that the rules of any monitoring should be regulated and employees should know on what terms their personal data are being processed. This has been required by the Labour Code since 2018, but there are still many entities that have not regulated in writing the purposes, scope and application of the monitoring in the organisation.

Also, the processing of employees' images in connection with video surveillance and the failure to provide access to personal data processed as part of it is the reason for frequent complaints to the President of the Personal Data Protection Office.

In addition, in each of the sectors indicated above, as in previous years, data subjects complained about the processing of their personal data without a legal basis, including the unauthorised sharing of their data with other entities.

Personal data of employees

Exercise of the right of access by the employer.

A former employee asked the company how it was processing his or her personal data. After 11 days, the company replied that the data were being processed in accordance with the law and therefore there was no cause for concern. However, there was no answer after a month either, hence the complaint to the President of the Personal Data Protection Office. The company explained to the President of the Personal Data Protection Office that the completion of the response was delayed due to reasons beyond control and was not due to bad intent. However, the company did not inform the former employee of such difficulties and disregarded the legal deadlines. This ended with a reprimand from the President of the Personal Data Protection Office.

This case illustrates the attitude of many entities processing personal data, for which data protection and compliance with GDPR requirements are secondary concerns. It is only the awareness of the consequences that an administrative proceedings for an infringement of regulations conducted against such entities can bring that serves as a motivating factor to align their data processing operations with the applicable law.

In 2023, the President of the Personal Data Protection Office noted that a significant portion of complaints also concerned the failure to fulfil information obligations under GDPR, including the failure to provide a copy of the data, pursuant to Article 15(3) GDPR. There were also numerous complaints about the incorrect implementation of the obligation to rectification of data and the incorrect implementation of the right to erasure of data under Article 17 of the GDPR and the right to object to the processing of data under Article 21 of the GDPR.

Some of such cases ended with a decision of the President of the Personal Data Protection Office to impose an administrative fine and an order to change the way personal data are processed.

The personal data of employees of a certain company were encrypted as a result of a ransomware attack. This company (the data controller) was unable to restore access to them. Moreover, the controller failed to notify the data protection breach to the President of the Personal Data Protection Office and failed to communicate it to the data subjects. The President of the Personal Data Protection Office imposed a fine on the company. The reason was not that the company had lost access to the data, but that it had failed to implement appropriate technical and organisational measures to ensure data security. Such measures should not only have been in place, but should have been regularly tested and their effectiveness assessed.

Loss of memory stick. During disciplinary proceedings, a lawyer sent a recording of a hearing containing personal data of eight individuals and information about their private lives on an unencrypted memory stick. The envelope tore, and the data carrier was lost. The President of the Personal Data Protection Office imposed a fine for failing to assess the risks to the data. The penalised individual filed a complaint with the Voivodeship Administrative Court in Warsaw, and the case is currently pending there.

The Voivodeship Administrative Court analysed cases concerning the processing of personal data in companies and issued the following decisions, among others:

The Voivodeship Administrative Court in Warsaw (II SA/Wa 714/23) upheld the decision of the President of the Personal Data Protection Office to reprimand a company for sharing **information obtained from a sick leave certificate, specifically that the complainant was pregnant, with other employees**. The Court agreed with the position of the President of the Personal Data Protection Office that the company had no legal grounds to process such data. It cannot be assumed that informing others about the reasons for the sick leave is necessary. An employer may process special categories of personal data of their employees, but health-related data are subject to the strict requirements of Article 9(2) of the GDPR.

In its judgment (II SA/Wa 2256/22), the Court agreed with the President of the Personal Data Protection Office that a **phone number constitutes personal data**, regardless of whether the entity has additional data or information identifying a specific person. This is yet another judgment confirming this position. The company had used the phone number to offer services and products. The President of the Personal Data Protection Office determined that

the complainant could not have reasonably expected his or her data to be processed for marketing purposes, as he or she had no connection with the company. The company erased the data, and the President of the Personal Data Protection Office issued a reprimand. The company appealed against this decision, claiming that a phone number does not constitute personal data, and therefore, the GDPR does not apply to the processing of such information. The court sided with the President of the Personal Data Protection Office, ruling that the company had processed personal data in the form of the complainant's phone number without a legal basis.

The Voivodeship Administrative Court in Warsaw (II SA/Wa 355/22) upheld the decision of the President of the Personal Data Protection Office that **the bailiff could process the complainant's data when notifying his former employer of the attachment of receivables**. The Court shared the position of the supervisory authority, holding that the bailiff processed the complainant's personal data in accordance with Article 6(1)(c) of the GDPR, i.e. for the purposes of the conducted enforcement - in order to fulfil his or her legal obligation.

Financial sector

Among the complaints against entities in the financial sector, invariably, compared to previous years, the largest number concerned **contracts with banks and credit institutions**.

In 2023, as in previous years, people complained to the President of the Personal Data Protection Office about the processing of their data related to the conclusion of various types of contracts, primarily credit agreements. Banks forwarded their claims against customers to debt collection companies, as well as to investment funds. The legitimacy of these claims cannot be assessed by the President of the Personal Data Protection Office, but it does check whether the rights of data subjects have been violated in the processing of data.

In 2023, the President of the Personal Data Protection Office also recognised complaints about the processing of personal data for the purposes of creditworthiness assessment and credit risk analysis by lending institutions. The problem was that financial institutions processed personal data by invoking banking secrecy (Article 105a(3) of the Banking Law), although they had no contractual relationship with the data subjects. They should therefore have had consent to process the data.

Processing of personal data by the bank from a scan of an identity card. A bank customer repaid a loan and asked for confirmation of this fact. The bank made the issuance of the certificate conditional on obtaining a scan of the identity card. In the opinion of the President of the Personal Data Protection Office, the bank should first consider whether it was necessary to obtain a scan of the person's ID card in order to fulfil the purpose of providing the data subject with information about the repaid loan. In the view of the President of the Personal Data Protection Office, there was no such need. Therefore, the data were processed in an unauthorised manner. Ultimately, this scan was deleted.

Processing of personal data by debt collection companies in order to enforce claims acquired through the assignment of receivables. Many proceedings concerned the processing of data in connection with the enforcement of claims. In such proceedings, the issue of making data available by the original creditor to another entity on the basis of receivables assignment agreements concluded pursuant to Article 509 of the Civil Code was often raised. It entails the entitlement to transfer the debtor's personal data enabling action to be taken to recover the debt. The President of the Personal Data Protection Office, in these proceedings, usually stated that such provision of personal data by creditors cannot be assessed as infringing the rights and freedoms of the data subject, who is a debtor. The person - as a debtor - has to reckon with the fact that when he or she defaults on an obligation, his or her right to privacy may be restricted due to the creditor's pursuit of financial obligations owed to him or her.

Processing of personal data by an insurance company in connection with the conclusion of a civil insurance contract. The complainant disposed of the insured vehicle during the course of the civil liability insurance without informing the insurance company of the sale, although such an obligation arises from the Act on Compulsory Insurance (Article 32(1)). The insurer notified the complainant that it renewed the contract, as it is obliged to do so. The President of the Personal Data Protection Office did not find any irregularities in the processing of personal data by the insurance company. The complainant's personal data were processed for the purpose of executing the insurance contract, and the correspondence was addressed to the complainant in connection with the obligation under the Act on Compulsory Insurance (Article 28).

Examples of cases that ended with a decision of the President of the Personal Data Protection Office to impose an administrative fine and an order to change the way personal data are processed.

Disclosure of personal data by an insurance broker. An insurance broker (data controller), wishing to enable its employees to work remotely, contracted a processor (performing IT services on its behalf) to implement such a solution. As a result of the changes made to the IT system, there was an unintentional publication of personal data involving a wide range of data. The case ended with the decision of the President of the Personal Data Protection Office to impose an administrative fine for an infringement consisting in the failure to implement appropriate technical and organisational measures to ensure the security of the processed data, which led to a breach of their confidentiality and accountability.

The Voivodeship Administrative Court analysed cases concerning the processing of personal data by financial institutions and issued, inter alia, the following decisions

In 2023, the Voivodeship Administrative Court in Warsaw (WSA) ruled on complaints against decisions of the President of the Personal Data Protection Office, which concerned the processing of personal data under Article 105a(3) of the Banking Law.

The Voivodeship Administrative Court (II SA/Wa 2198/22) held that interpreting the obligation to inform the data subject solely on the basis of the provisions of the Civil Code

is incorrect. In the Court's view, the correct interpretation of the phrase 'informing that person' contained in Article 105a(3) of the Banking Law should take into account not only the content of the provision contained in Article 61(1) of the Civil Code, but also that part of the provision contained in Article 105a(3) of the Banking Law which establishes an additional thirty-day period for the performance of the obligation. Since it is the bank that derives legal consequences from notifying the participant of its intention to process his or her personal data constituting bank secrecy without his or her consent, the bank must prove that 30 days from the date of informing him or her of this intention have expired without effect. Demonstrating this circumstance, however, requires an indication of the beginning of this 30-day period.

The Voivodeship Administrative Court (II SA/Wa 1554/22), in dismissing the appeal against the decision of the President of the Personal Data Protection Office, indicated that the possibility of the addressee becoming acquainted with the content of the statement cannot be equated with the addressee actually becoming acquainted with the statement (the fact of becoming acquainted). The Court found that the scans (pdf files) of the statement with the indicated tracing number and date of sending as well as an excerpt from the electronic sending book did not allow to conclude that the bank informed (made it possible to become acquainted with the information in the ordinary course of events) the data subject of its intention to process his/her personal data pursuant to Article 105a(3) of the Banking Law.

The problem of public service providers

Public institutions are digitally processing data on a large scale that they previously processed in a traditional way. Given the magnitude of this phenomenon, the risks for data subjects are increasing.

A worrying trend in Poland is the creation of regulations providing for large-scale processing of personal data or leading to the merging of different databases and registers, without a thorough analysis of all aspects of the processing. Including without assessing the risks involved.

It is necessary to review the provisions on the use and publicity of the personal identification number (PESEL number), which is a national identification number within the meaning of the GDPR.

In 2023 the President of the Personal Data Protection Office pointed to this problem, among other things, when giving its opinion on the draft act amending the act on public statistics or in a request to the President of the Board of the National Council of Chambers of Agriculture (personal identification number is disclosed at the seat of the commune in the register of members of the chamber of agriculture entitled to vote in elections to the general meetings of the chambers of agriculture).

Examples from the operation of the President of the Personal Data Protection Office show what a challenge we face.

Health care

The health care system collects detailed personal data about us, which constitute special categories of data (e.g. health data). From the complaints received by the President of the Personal Data Protection Office, it is clear that these data are either used by unauthorised persons or are processed for inappropriate purposes. It will take a lot of effort to spread awareness that this is an illegal activity.

An example is the complaints against doctors and employees of doctors' offices who, in various non-medical life situations, illegally obtained personal data they needed from the Electronic Services Platform of the Social Insurance Institution (PUE ZUS).

A doctor obtained the data of a witness in a civil litigation with Electronic Services Platform of the Social Insurance Institution. In a libel suit brought by a doctor against a journalist (and the doctor won the case), a woman who claimed to have been a patient of this doctor testified as a defence witness. The doctor filed a notice of false testimony: the woman had never been treated by him. The doctor obtained the woman's data from PUE ZUS. He took the position that he was acting for the purposes of the pending criminal proceedings and therefore for his legitimate interest. The President of the Personal Data Protection Office noted that a doctor's legitimate interest may be a professional purpose or one related to professional activity. In the President of the Personal Data Protection Office's view, the doctor was not entitled to use personal data from the PUE ZUS for the purposes of litigation. The case ended with a reprimand.

The doctor checked the data of his child's mother, with whom he is in conflict, in the PUE ZUS. He checked whether she actually had sick leave to care for their child. He explained that a year and a half ago the child's mother had cut him off from information about the child, including the child's health. PUE ZUS was the only way to find out if the child was ill. Unfortunately, no regulations allow such processing of personal data. The case ended with a reprimand.

An employee of a doctor's office was confirming in the PUE ZUS whether he had the correct address details of a friend. The data controller considered that this conduct was explained by the 'family situation'. However, in the opinion of the President of the Personal

Data Protection Office, this was a violation of GDPR. Access to the data collected on the PUE ZUS profile was not related to the provision of a medical service to the complainant.

A medical assistant accessed the PUE ZUS from a doctor's account at a clinic and checked whether an absent employee had sick leave. The person whose data was checked complained to the Personal Data Protection Office that there was no basis for looking into his/her account. The person did not have a medical appointment that day. The President of the Personal Data Protection Office noted that in order to use the PUE ZUS, one has to have an account and have a defined role in it. He considered it unacceptable to use a doctor's account to check employee's data. The President of the Personal Data Protection Office issued a reprimand to the clinic.

The doctor checked the data in the PUE ZUS for matters related to the employment affairs of another person. They both worked for the same company and were not bound by the doctor-patient relationship. The doctor was also not the complainant's actual employer - it was the company, which did not authorise the doctor to act in this way. As it turned out, the situation occurred because the person authorised to act on behalf of the payer of ZUS (social insurance) contributions was absent. The President of the Personal Data Protection Office admonished the doctor that taking advantage of the doctor's capacity in a situation where he or she is performing tasks for the employer, and without authorisation, is not appropriate.

Prescriptions and medical referrals issued by unknown doctors. People complained that their Internet Patient Account (IKP) showed that they had been issued with prescriptions or referrals by doctors they did not know. These orders had the status of being executed, while the erroneous entries and prescriptions were distorting their medical histories. In the course of the investigations, the controllers (medical facilities, doctors) indicated that the prescriptions/referrals were issued, among other things, as a result of a mistake and erroneous verification of the patient. However, according to the President of the Personal Data Protection Office, this was not a minor error. It occurred as a result of negligence of the duties incumbent on the data controller. These cases ended with reprimands.

Schools and Universities

Schools and educational establishments hold personal data about children and young people, as well as their guardians. If one does not think in terms of the risks to these data - and to the data subjects - it is easy to run into problems.

The scale of the problem is shown by complaints and questions to the President of the Personal Data Protection Office. In 2023, these included issues such as the legality of entering into entrustment agreements between the policyholder and the school as the insured, the processing of pupil's personal data within the framework of occupational medicine, the retention by schools of original certificates of pupils confirming the completion of a given stage of education, the processing of a pupil's image, the processing of

graduates' data or the withdrawal of a pupil's consent to the processing of his or her personal data by the school.

Consequences of incorrect anonymisation of personal data when disclosing public information.

The mother of a pupil complained to the Superintendent about irregularities at the school. The Superintendent carried out an ad hoc inspection and the minutes were made available on the school's Public Information Bulletin. It contained the complainant's data: her first name, the beginning of her surname and the information in which class her child was studying. The anonymisation was therefore ineffective - the person's data could easily be established. The President of the Personal Data Protection Office assessed that the school, by making the minutes available in a pseudonymised version, breached the principle of data minimisation set out in Article 5(1)(c) of the GDPR. The disclosure of the data was not adequate, relevant or limited to the purpose for which they were processed (in this case, the sharing of information on the results of the inspection).

Disclosure of a minor's personal data on an online group to unauthorised persons. A kindergarten provided a list of accepted children on an online group. One child had an 'o' next to his or her name. According to his or her guardian, the kindergarten thus revealed that the child had a disability certificate and special education needs. The kindergarten explained that the list was published by the teacher himself or herself, it was not accompanied by a legend, so the 'o' on it could mean many different things (observation, opinion, certificate or need for extra rest – *translator's note: these are translations of the Polish words starting with an 'o'*). The President of the Personal Data Protection Office pointed out that it is the responsibility of the kindergarten to publish the list, and that publishing it in a closed online group does not fulfil the obligation to publicly announce the list of admitted children. On the other hand, the letter 'o' could not be unambiguously linked to a specific category of personal data. Due to the fact that the list of children admitted to the kindergarten was removed on the same day as the day of its publication, the President of the Personal Data Protection Office decided that it would be sufficient to apply a reprimand to the kindergarten.

A youth educational centre (MOW) is claiming food dues from the person who brought the minor. The MOW decided to claim the juvenile's food dues from the person who brought him or her to the centre. However, this person was not the legal guardian of the juvenile. The President of the Personal Data Protection Office did not find an irregularity here, as the personal data were only provided to the court, which could assess in this situation who was responsible for the juvenile. The court recognised the MOW's position. The applicant could have exercised his or her rights and filed an objection to the payment order issued by the district court. The data protection provisions do not apply in this case.

Examples of cases that ended with a decision of the President of the Personal Data Protection Office to impose an administrative fine and an order to change the way personal data are processed.

A public university accidentally disclosed online the data of candidates for trips organised as part of an international student exchange. This happened because the registration application was not properly secured, not to mention the lack of regular testing of the effectiveness of these safeguards. The breach was notified by a controller (the university). The incident occurred following an error as part of development work to move the application to a new production server. The incident led to unsecured data being indexed by one of the search engines.

The President of the Personal Data Protection Office emphasised in the justification of the decision that the controller was not able to demonstrate during the proceedings that the data security measures it had implemented were adequate in view of the potential risks. The President of the Personal Data Protection Office imposed a fine on the university. The latter has appeal against this, and the appeal is pending before the Voivodeship Administrative Court in Warsaw.

The problem of public institutions and state policies

In 2023, in cases concerning the activity of the Police the President Personal Data Protection Office received **1,328 complaints against the public sector**. An example of the problems faced by public institutions is the disclosure of personal data on the pages of Public Information Bulletins. The demarcation between the right of access to public information and the right to privacy is something that requires more care from the public institution.

Another serious issue is the answer to the question of how much and what kind of data the state can collect. There is no doubt that data-driven public policies are better and more effective. However, data processing always involves risks for data subjects - so the question is whether it is justified.

Right to public information and right to privacy

Disclosure of personal data in a resolution published on the Public Information Bulletin. The commune made the applicant's data available on the BIP with the information that his or her offer did not meet the formal requirements for the post of deputy chief accountant. The commune authorities believed that they had to do so because the councillors, when adopting the resolution on the recruitment for the post with the complainant's data, also decided that this information would be made public.
The President of the Personal Data Protection Office, in issuing a reprimand to the mayor, recalled that the right to public information is subject to restrictions, inter alia, due to the privacy of the individual. The resolution could have been published by anonymising the personal data.

Disclosure of personal data on the Public Information Bulletin in relation to the publication of the minutes of the Poviat Council session. A citizen complained to the Poviat Starosty that the headmaster of a school did not want to pay her pension and severance pay. The

Poviat Council dealt with the complaint during a session and the minutes of the meeting included the complainant's data. The document was disclosed under the provisions on access to public information. In admonishing the Staroste, the Personal Data Protection Office stressed that there was no reason for the complainant's data to be published on the Public Information Bulletin. Therefore, there has been a breach of GDPR. What was important in this case was that before the President of the Personal Data Protection Office issued his decision, the Poviat Starosty had removed the applicant's data from the Public Information Bulletin website.

Disclosure of the data of the whistleblower to the parties to the administrative proceedings. The complainant informed the mayor of a violation of the Environment Protection Act in connection with the felling of trees. The mayor initiated proceedings and issued an administrative decision. In it, he informed that he had received the complaint and provided the complainant's data, although she was not a party to the administrative proceedings. The President of the Personal Data Protection Office indicated that such an action did not find a basis in the provisions of the Code of Administrative Procedure, which allow for the investigation of irregularities signalled by citizens by initiating proceedings ex officio, without the need to disclose the source of the information obtained. The President of the Personal Data Protection Office issued a reprimand to the mayor.

Examples of consecutive cases that ended with the decision of the President of the Personal Data Protection Office to impose an administrative fine and an order to change the way personal data are processed.

Disclosure of a doctor's personal data by the Minister of Health. The Minister of Health disclosed a doctor's data on the X platform in 2023, along with the information that he or she had written a prescription for psychotropic and painkiller drugs on himself or herself. The data came from the Electronic Platform for the Collection, Analysis and Sharing of Digital Resources on Medical Events and were transmitted via WhatsApp messaging. The President of the Personal Data Protection Office imposed administrative fine on the Minister of Health for, among other things, the unlawful disclosure of the doctor's data.

Lost memory sticks from a court. A District Court’s employee lost three memory sticks (one official - encrypted and two unencrypted - private) with the data of an undetermined number of people. The President of the Personal Data Protection Office proved an infringement in the proceedings, for which it imposed a fine. The infringement consisted in the Court's failure to implement appropriate technical and organisational measures ensuring a level of security corresponding to the risk of data processing using portable memory sticks. The Court's risk analysis prior to the infringement shows that the data controller foresaw the risk of loss of confidentiality through loss of data on unprotected memory stick and implemented appropriate safeguards. However, it did not foresee that the data would be moved to private, unsecured memory stick and then lost. The President of the Personal Data Protection Office indicated that it would be worth introducing a blockade for private memory sticks or making their encryption mandatory. The Voivodeship Administrative Court

in Warsaw, after a complaint from the Court, upheld the decision of the President of the Personal Data Protection Office.

The Ministry of Foreign Affairs notified the Regional Court in Krakow that the consul in the UK had received a damaged delivery containing the personal data of several people. The envelope was torn and anyone could have seen the data. The documents were sent at the request of the Court, which was their controller. The Court did not notify this breach of data to the President of the Personal Data Protection Office and did not communicate it to the persons whose data were in the documents. The President of the Personal Data Protection Office pointed out that the Court's Data Protection Officer had wrongly assessed that the risk to the data was not high because the envelope had torn in the UK and the documents were in Polish. The President of the Personal Data Protection Office noted that today there are tools available to translate texts quickly and the Polish community in the UK is numerous, so the case cannot be explained in this way. The President of the Personal Data Protection Office issued a decision to impose an administrative fine. The decision is not final and awaits the assessment of the Voivodeship Administrative Court in Warsaw.

The District Public Prosecutor's Office handed over the non-anonymised documents to the journalist at his or her request. The breach concerned the data of three persons, including a child, and the controller did not notify it to the President of the Personal Data Protection Office and did not communicate it to the persons concerned. Subsequently, the controller (i.e. the District Public Prosecutor's Office) refused to open an investigation into the data protection breach, considering that it had not occurred. In the course of the administrative proceedings, the President of the Personal Data Protection Office found that the District Public Prosecutor's Office had not carried out a data protection risk analysis, so its claim that the breach had not occurred was not substantiated. The mere refusal to initiate proceedings is not a sufficient basis for such a conclusion under the GDPR. The Voivodeship Administrative Court in Warsaw upheld the decision of the President of the Personal Data Protection Office to impose an administrative fine.

Examples of cases involving public institutions in which the Voivodeship Administrative Court in Warsaw has ruled in 2023

The Voivodeship Administrative Court in Warsaw (II SA/Wa 1944/21) and then the Supreme Administrative Court (III OSK 595/22) upheld the decision of the President of the Personal Data Protection Office ordering the mayor to remove from the recording of the municipal council session on the website, the personal data of the complainant in terms of name. The Voivodeship Administrative Court shared the position of the President of the Personal Data Protection Office that in the present case the exemptions from the Act on Access to Public Information do not apply, as the personal data disclosed in the recording do not concern a person performing a public function, nor did the complainant waive his right to privacy. The Supreme Administrative Court clarified that the Act on Access to Public Information excludes the recognition as persons performing public functions of such persons who are known to the public (nationwide or to a specific regional or local community), but who remain outside the structures of the state apparatus.

The Voivodeship Administrative Court in Warsaw (III OSK 595/22) upheld the decision of the President of the Personal Data Protection Office to admonish a controller who had breached the principle of data minimisation by collecting documents in the complainant's personal file that were in fact unnecessary for the purpose of processing (on the postal envelope, in addition to the complainant's name, surname and address, there was also his official position and place of work).

The Voivodeship Administrative Court in Warsaw (II SA/Wa 446/23) upheld the President of the Personal Data Protection Office's reprimand to the mayor of a city for disclosing the number plate of the complainant's vehicle (a person performing a public function) during a session of the city council. The Court shared the view of the President of the Personal Data Protection Office that the number plate of the complainant constitutes his or her personal data in these proceedings, as his or her name and surname were disclosed at the same time.

Border authorities

The Schengen Information System (SIS) is the most efficient tool to ensure effective cooperation between immigration authorities, police, customs and judicial authorities in the EU and Schengen associated countries. It allows data to be entered and viewed on wanted persons, persons who may not have the right to enter or stay in the EU and missing persons - particularly children. Following a change in the law, so-called 'preventive alerts' can be entered into it - authorities in Member States can identify children where the risk of abduction is particularly high. These changes mean that border guards and law enforcement services will be alerted when there is a high risk of imminent abduction of a child by one of the parents and will be able to investigate the circumstances of such a child's journey more thoroughly, applying protective custody to the child if necessary. Following the amendment of these provisions, President of the Personal Data Protection Office carried out a sectoral inspection of how data on children are collected and processed. The inspection did not reveal any problems.

The Police and uniformed services

In 2023, the President of the Personal Data Protection Office supported the Police's arguments and has not intervened in cases involving the protection of personal data, although it has checked the extent of their processing by the Police and analysed complaints against uniformed officers.

Processing of personal data in the National Police Information System (KSIP). In this system, the Police collect all data on persons of interest to them. The database contains information on persons convicted of various offences and retains knowledge of this even when the offence itself has been expunged. The President of the Personal Data Protection Office therefore gets many complaints from people whose data the Police did not want to remove from the KSIP, even though they requested it. Although the Police collect personal data for the KSIP in accordance with the law, the President of the Personal Data Protection

Office noted that this does not mean that the data can be processed indefinitely. Under the provisions of the current Act on the protection of personal data processed in connection with preventing and combating crime, personal data processed are subject to periodic review and erasure in the event that further processing is deemed inappropriate. The Commandant-in-Chief of the Police is required to verify personal data at least every 10 years. It is to check whether there is data whose further storage is unnecessary. At the same time, in 2023 the President of the Personal Data Protection Office acknowledged the arguments of the Police that they still need specific data 'in connection with the infringement of the provisions of criminal law by the complainant and the type of the provisions violated'.

Provision of personal data by the Police to the Sanitary Inspectorate of a person who did not cover his or her mouth and nose with a mask. This concerned situations from the time of the coronavirus pandemic: police officers asked persons without masks to present their IDs and then provided their data to the Sanitary Inspectorate. The Sanitary Inspectorate could fine such persons up to PLN 30,000 in administrative proceedings. The question, however, was whether the Police had the right to pass on these data to the sanitary inspectorate.

The Ombudsman for Human Rights took the position that it did not, because a police note is not a document issued by an authority, and only such a document can be used in administrative proceedings. Therefore, the Ombudsman for Human Rights challenged administrative fines imposed on citizens on the basis of police notes before the administrative courts.

The President of the Personal Data Protection Office has taken a similar position: The Police have no grounds to provide personal data to the sanitary epidemiological service. However, it considered that the sharing of personal data with the Sanitary Inspectorate had already taken place and was an irreversible process, and therefore refused to grant the complainant's request in 2023.

Data Protection Officers and their role

Data Protection Officers (DPOs) play a key role in creating an effective system of personal data protection in Poland and across the European Union. They are the ones who support controllers in the implementation of their obligations concerning personal data protection. They also operate as a point of contact for data subjects and the supervisory authority.

At the same time, DPOs have the right to request consultation with the President of the Personal Data Protection Office. Therefore, cooperation with Data Protection Officers is extremely important for the President. DPOs' questions are an important source of knowledge about the problems they face. The DPOs accurately identify legal problems resulting, for example, from gaps in regulations or their inadequate interpretation. In such situations, the DPOs expect the Personal Data Protection Office to provide guidance or to take appropriate action, e.g. directing a legislative intervention.

In 2023, the Personal Data Protection Office received **253 questions from Data Protection Officers**. The President of the Personal Data Protection Office provided **246 answers**. The slight decrease in the number of questions (there were 274 questions in 2022, 301 in 2021) may be due to the fact that many issues were clarified in previous years.

With each passing year, the DPOs' questions are less and less concerned with basic issues, and rather with more complex problems involving irregularities and risks that may affect the independence of the Data Protection Officer and the effective performance of its functions (e.g. the DPO's role as a representative of the controller). Data protection officers are very sensitive in identifying threats to the protection of personal data arising from legal loopholes or imprecisely drafted laws or their incorrect interpretation.

The first group of questions from DPOs covered issues that have invariably arisen for several years. These include the existence of conflicts of interest in relation to the performance of the function of DPO, the determination of the status of entities involved in the processing of personal data, the disclosure of personal data, or problems with the practical application of both personal data protection provisions and sectoral legislation.

The second group of questions concerned in 2023 current events and issues, such as the status of entities processing personal data for the organisation of parliamentary elections, or issues related to the processing of personal data in connection with the application of the provisions of the Act on Support for the Development of Digital Competences of Students and Teachers, which came into force in 2023.

The President of the Personal Data Protection Office responded to them on the Office’s website or in the Personal Data Protection Office’s Newsletter for DPOs, the subsequent Personal Data Protection Office’s Bulletin. The President also signalled to the relevant entities the observed irregularities or the need for legislative changes.

An important problem is that data controllers (employers) impose additional duties on DPOs that may hinder them from performing their data protection tasks. The DPO cannot be responsible for performing the controller's task, e.g. notifying breaches, and at the same time monitor whether this task is performed correctly. Such a situation may arise, for example, when a DPO is granted a power of attorney to represent the controller in matters relating to personal data protection. This is because the task of the DPO is to inform the controller of the controller's obligations under the GDPR and to monitor the fulfilment of these obligations (Article 39(1)(a) and (b) GDPR). Acting as a representative of the controller with regard to the obligations imposed on the controller may make it significantly difficult or impossible for the DPO to independently assess whether the controller's obligations are being implemented at all and whether they are being carried out correctly.

It is worth to know that in 2023, the situation of DPOs was analysed by the European Data Protection Board of the European Data Protection Regulation (EDPB - more on the cooperation of the President of the Personal Data Protection Office with the Board below). The President of the Personal Data Protection Office submitted the following identified Polish problems concerning DPOs to the EDPB report:

- burdening the DPO with the controller's responsibilities, e.g. running the register of processing operations,
- concluding an agreement on entrustment of personal data processing between the controller and the DPO,
- granting the DPO a power of attorney to represent the controller in matters of personal data protection,
- providing by companies employing DPOs the services of outsourcing DPO's functions and at the same time the services of performing the so-called 'GDPR implementation' for the controller.

In its report, EDPB stated that more awareness raising, information and enforcement activities need to be carried out in all countries (this should be done by supervisory authorities such as the President of the Personal Data Protection Office). DPOs should have enough opportunities, time and resources to refresh their knowledge and learn about the latest developments.

Codes of conduct and accreditations

The GDPR (Article 40) is the basis for the drawing up of codes of conduct, which aim to clarify and assist in the application of the GDPR in the industry concerned.

The drawing up of a code of conduct is a lengthy process, requiring hard and meticulous work. Those interested may wish to refer to the Report as it enumerates the mistakes that can be avoided in this work.

There are many benefits of adopting the code. It is not only the guarantee of certainty of application of certain solutions approved by the supervisory authority. Controllers can also count on supervision of their personal data processing operations by an independent body monitoring the code.

Such monitoring bodies, in order to be accredited by the President of the Personal Data Protection Office, must demonstrate that they are independent of the author of the code and that they have adequate resources to fulfil their role.

So far, the President of the Personal Data Protection Office has approved two codes. The first one was approved in 2022. "Code of conduct concerning the protection of personal data processed in small medical facilities" developed by the Federation of Healthcare Employers' Unions (FZPOZ)) Zielona Góra Agreement. Accreditation for monitoring its application was granted to Jamano company. And in 2023, the supervisory authority approved the Code of Conduct for the healthcare sector, prepared by the Polish Hospital Federation, and granted accreditation to KPMG Advisory company to monitor compliance with its provisions. The document is the first code in Europe to cover public and private entities in the medical sector.

In the network of European institutions

The President of the Personal Data Protection Office cooperates with other supervisory authorities. This cooperation provides better guarantees for data protection in Europe than acting alone and ensures that the GDPR is applied uniformly across EU countries.

The cooperation network is crucial for complaints about cross-border data processing. This is because such complaints are handled by the supervisory authority in the country where the controller (the entity complained against) is established or represented. Through extensive cooperation and collaboration of all supervisory authorities in the field of personal data protection, the handling of cross-border complaints has, in the opinion of the President of the Personal Data Protection Office, a significant impact on the greater awareness of complainants to exercise their rights.

Cases involving controllers such as Meta and Twitter are within the jurisdiction of the Irish supervisory authority (Data Protection Commission), as these companies are represented in Ireland. For this reason, the Irish authority is the lead supervisory authority in cases of breaches of data protection laws in relation to individuals located in the EU. Proceedings against so-called ‘tech giants’ always cause a greater public rift, which affects people's awareness.

It should be noted that while cooperation with the German supervisory authorities as well as with the French or Irish supervisory authorities is functioning smoothly, contact with the Italian, Luxembourg and Dutch supervisory authorities was sometimes difficult in 2023, inter alia due to differences in the applicable national procedures in the proceedings conducted.

In 2023, cross-border complaints mostly concerned the implementation of the complainants' rights in relation to controllers offering access to social networking sites such as Facebook and Instagram, in particular regarding the right of access to data and the right of erasure, as well as the failure to communicate transparently with the controller or to provide a timely response to the requests included in Chapter III of the GDPR. In the proceedings, initiated by complaints received in 2023, controllers usually provided comprehensive answers to the questions asked and did not hide possible data breaches, often explaining them by human error.

User accounts on large social media platforms

Many complaints in 2023 related to the activities of large social media platforms. These concerned:

- the inability to access or erase personal data,
- failure to communicate transparently with the controller, and
- requests for excessive amounts of data to verify the identity of users of these platforms, such as scans of identity documents.

Here it is worth pointing out that in order for the assistance of the President of the Personal Data Protection Office (as well as other data protection authorities in Europe) to be effective, it must be demanded of it not to restore the account or functionality. This is beyond its control. If an account has been deleted/blocked, the President of the Personal Data Protection Office can only intervene on the personal data on the account. The task of the President of the Personal Data Protection Office is to assess the processing of personal data, not issues related to the handling of user accounts of websites and applications.

So how should complaints be formulated? This was demonstrated in the case of the deletion of an account on Instagram. The complainant indicated that the administrator of the portal had wrongfully taken away his access to his Instagram account. And it was connected to the complainant's gainful activity. Thus, he lost contact with contractors and trust built up over the years. The President of the Personal Data Protection Office referred the complaint to the Irish supervisory authority (Data Protection Commission - DPC). However, the DPC did not take up the case because, like the President of the Personal Data Protection Office, it has no jurisdiction over the restoration of accounts.

However, the DPC has sent a “checklist” of the elements it believes a cross-border data complaint should contain. The complaint should include:

1. a copy of the request to the controller to comply with the data subject's rights, including the date of the request.

2. a copy of the controller's response (if it came) with the date of the response.

3. evidence of whether the controller has taken a two-month extension of the time limit for complying with the request under Article 12(3) of the GDPR and, if so, an indication of the date on which the controller informed the data subject of the extension.

4. details of any additional information required by the controller to verify the identity of the data subject pursuant to Article 12(6) GDPR.

5. copies of any other correspondence between the data subject and the controller in relation to the request to comply with the data subject's right.

6. copies of any relevant correspondence between the supervisory authority concerned and the data subject and the controller, where applicable, in relation to the request to comply with the data subject's right.

7. a copy of the data subject's complaint to the supervisory authority concerned, showing the date of the complaint.

8. translated documents for each of the above, if required.

The DPC has indicated that the checklist is intended to provide other DPAs with a guide to the information and/or documents that the DPC needs in order to assess and progress potential cross-border complaints in respect of a data subjects rights related request made pursuant to Articles 15-22 of the GDPR.

The Irish supervisory authority has asked the President of the Personal Data Protection Office to review each complaint against an entity established in Ireland against the above checklist.

Cooperation between supervisory authorities in the context of the investigation of a local case. One case involved a controller with a branch in Romania failing to comply with a complainant's request to delete his or her personal data. In cooperation with the Romanian supervisory authority, the President of the Personal Data Protection Office managed to establish that the case only concerned the Romanian branch and only affected data subjects in Romania. The case was therefore handled locally by the Romanian supervisory authority on the basis of Article 56(2) GDPR. The complainant only signed contracts with the Romanian branch of the bank and the case was of an individual nature and concerned incorrectness in the processing of the complainant's data.

Requests from other supervisory authorities

In accordance with the cooperation mechanism regulated in Chapter VII of the GDPR, Section 1, supervisory authorities shall provide each other with relevant information and mutual assistance for the consistent implementation and application of the GDPR and shall put in place measures for effective mutual cooperation. Mutual assistance shall include, in particular, requests for information. Authorities shall exchange information through the Internal Market Information System (IMI).

In 2023, the President of the Personal Data Protection Office received **27 requests from supervisory authorities from other countries**, including: France, the Netherlands, Slovenia, Slovakia, Italy, Liechtenstein, Finland, Norway, Ireland, Malta, Germany, Denmark, Cyprus. By comparison, 41 such requests were received in 2022, 25 in 2021, and 14 in 2020.

Cooperation within the EDPB

One of the statutory tasks of the authority competent for the protection of personal data is participation in the works of international organisations and institutions dealing with the issues of personal data protection. The tasks of the President of the Personal Data Protection Office include cooperation with supervisory authorities of other EU Member States, in particular as part of the activities of the European Data Protection Board (EDPB).

Detailed data on the cooperation between the President of the Personal Data Protection Office and the EDPB can be found in the Report for 2023. We would like to point out that in 2023 the EDPB has prepared, inter alia:

- a guide to data protection for small businesses;
- a model complaint form to facilitate the submission of complaints by individuals and the subsequent handling of complaints by supervisory authorities in cross-border cases;
- coordinated law enforcement tasks for the use of cloud services by the public sector.

EDPB taskforces

In 2023, the Personal Data Protection Office's employees also represented the Polish supervisory authority in EDPB taskforces and networks, among others:

- the 101 Complaints Taskforce, which deals with complaints submitted by NOYB. The complaints concern companies in 30 EU and EEA Member States in connection with the use by controllers of tools by means of which data are transferred to third countries in a manner inconsistent with the judgment of the CJEU in case C-311/18 (Schrems II), which decided when the transfer of data to third countries is legal;
- Taskforce on ChatGPT;
- Taskforce on the Interplay between Data Protection, Competition and Consumer Protection Law;
- Cookie Banner Taskforce.

The EDPB and national supervisory authorities are actively cooperating in their respective responsibilities to ensure effective oversight of large-scale information systems and the Union's authorities and organisational units. Coordinated activities include, among other things, joint inspections and investigations and work on a common methodology.

In 2023, representatives of the Personal Data Protection Office participated in the following meetings:

- the Customs Information System (CIS) Supervision Coordination Group, which helps to prevent, investigate and prosecute customs and agricultural law violations;
- the Visa Information System (VIS) Supervision Coordination Group;
- The Eurodac Supervision Coordination Group, which contains the fingerprints of all registered asylum seekers in EU Member States and cooperating countries.

The representative of the Personal Data Protection Office also participated in the work of the Coordinated Supervision Committee (CSC) covering the supervisory activities of the Schengen Information System (SIS II), as well as the Internal Market Information System (IMI), Eurojust and Europol.

EDPB's binding and urgent decisions:

The EDPB is not only a forum for developing positions and analysing issues. It can, in urgent and emergency situations, react using the right given to it by Articles 65 and 66 of the GDPR. In 2023 the EDPB adopted two binding decisions under Article 65 GDPR and one urgent decision under Article 66 GDPR.

In April 2023, the EDPB resolved a dispute over a fine imposed on Meta Platforms Ireland Limited (Meta) and a data processing compliance order in Binding Decision No. 1/2023. The Board instructed the Irish supervisory authority to amend the draft decision and impose a fine on Meta**.** On this basis, the Irish supervisory authority imposed a fine of €1.2 billion on Meta for its transfer of personal data to the US under standard contractual clauses. Meta was required to comply with the provisions of the GDPR for its data transfers.

In August 2023, the EDPB resolved a dispute over the Irish supervisory authority's draft decision on the processing of personal data of users aged 13 to 17 by TikTok Technology Limited (TikTok IE). Following a binding decision by the EDPB, the Irish supervisory authority issued a final decision finding that TikTok IE breached the fairness principle of the GDPR when processing personal data relating to children aged 13 to 17 and issued a reprimand, a compliance order and a €345 million fine.

Following EDPB Binding Urgent Decision No. 1/2023 of 27 October 2023, the Irish supervisory authority adopted a final decision on 10 November 2023, imposing a ban on Meta's processing of personal data for behavioural advertising purposes on the legal bases of contract and legitimate interest. The EDPB's binding urgent decision followed a request from the Norwegian supervisory authority to take final measures that would apply across the European Economic Area (EEA). Initially, the Norwegian supervisory authority imposed a three-month ban on the processing of personal data of Norwegian citizens for the purpose of behavioural advertising. The ban only applied within Norway. The EDPB led by its action to extend the ban to the whole EEA.

European law and the comments of the President of the Personal Data Protection Office on Polish legislation

Rulings of the Court of Justice of the European Union are also important for data protection. The CJEU studies situations in various EU countries and analyses different solutions - its positions imply the necessity of reviewing Polish law for adaptation to its rulings and EU regulations. The CJEU defends the rights of Polish citizens.

Although the questions posed by the courts of the Member States to the CJEU in 2023 concerned a variety of topics, it can be noted that they were most often related to the controller's obligations towards data subjects and the right to erasure or rectification of data. They were largely due to the intensive development of the information society and technological progress, which translated into questions on the interpretation of the provisions of the GDPR in the light of new technological developments.

Of the cases that were decided by the CJEU in 2023, the majority, in the opinion of the supervisory authority, did not require changes to Polish law. It did, however, affect the interpretation of the legislation. Only with regard to the judgment in Case C-252/21 Meta Platforms et al./Facebook e.a., did the President of the Personal Data Protection Office state the need to amend the legislation. The judgment in this case is precedent-setting as it concerns the necessity of interaction between the competition authority and the personal data protection authority when the same case concerns both consumer rights and personal data protection. Therefore, in its position, the supervisory authority considered it important to discuss and consider the adoption of national legislation resolving the issue of cooperation between the supervisory authority and the competition authority in order to avoid competence disputes and dualism of decisions.

Polish law and challenges

While analysing the judgments of the CJEU and questions referred for a preliminary ruling to the CJEU from other countries (see the Report), as well as the provisions of the GDPR, the President of the Personal Data Protection Office may comment on the legislation being prepared. He may also indicate the need for changes in the legislation before the responsible institutions notice it.

The legislator does not ask the President of the Personal Data Protection Office for its opinion

Unfortunately, also in 2023, public authorities failed to include the Personal Data Protection Office in the consultation process when working on new legislation. Therefore, important draft normative acts concerning the processing of personal data or containing regulations in this area did not reach the assessment of the President of the Personal Data Protection Office. This is not only an action against the applicable regulations and obligations, but also a missed opportunity for expert support of the drafter by the supervisory authority at the earliest possible stage of the legislative process. In a large number of cases, drafts that are not consulted with the President of the Personal Data Protection Office at the legislative stage of the government's work are later referred to it for an opinion/position by the Sejm and the Senate.

The legislator fails to do a privacy test

The provisions of the GDPR require that any processing of personal data must be planned taking into account the concept of data (and privacy) protection at the design stage (*privacy by design*) as well as at the time of the processing itself.

When the legislator envisages that the processing of personal data will be carried out using certain IT solutions, it should take into account from the outset the impact that their use will have on the privacy of the data subjects. In doing so, it should also take into account:

- the state of the art,
- the costs of implementation, and the nature,
- the scope, context and purposes of data processing,

At the same time, it should design the envisaged digital solutions in such a way that they are appropriate to the specific case and, at the same time, free from any risks of breaches of data subjects' rights and freedoms at the highest possible level.

Education

Although Polish citizens are increasingly aware of the risks in the area of personal data protection, many still do not know how to react properly in the event of data loss. They are also unable to foresee the negative consequences of such an event. In addition - the rapid development of new technologies continues to present us with new challenges.

Therefore, for the President of the Personal Data Protection Office, educational activities are an extremely important part of its activity. It undertakes wide-ranging information and educational activities, the diverse form and dynamics of which contribute to raising citizens' awareness. Examples are as follows:

The “Your data - Your concern” educational programme is the flagship undertaking of the Personal Data Protection Office, on a nationwide scale. It engages entire school communities, teaches young and old, and reaches out to students, teachers, principals, parents and even seniors. On average, each year the programme hosts several thousand lessons and various events aimed at students, teachers, parents, seniors and the local community. Around 50,000 students participate in each edition of the programme and more than 5,000 teachers are involved. The programme organises webinars in the series “GDPR in the school bench” for school principals, teachers and school data protection officers, as well as webinars for primary and secondary school children (“What bait will you fall for?”) and early childhood education students (“With the GDPR-buddy we protect personal data” – *In Polish the GDPR-buddy is called “Roduś”*). More than 4,000 socially valuable projects for the protection of children's personal data have been created, the most interesting of which have been awarded in competitions organised by the President of the Personal Data Protection Office. Therefore, we see as a challenge for the coming years the development of this project and reaching an increasingly large audience with it.

The Personal Data Protection Office has developed guides, guidelines and manuals for DPOs as part of its activities with the supervisory authorities of other countries.

The President of the Personal Data Protection Office cooperates with universities and the Office's experts support important events aimed at different audiences, including data protection officers, with their knowledge.

Webinars addressed to DPOs presented the public's expectations towards DPOs and the controller's obligations, such as the implementation of appropriate technical and organisational measures to ensure data security and compliance of data processing with the provisions of the GDPR.

In 2023, experts of the Personal Data Protection Office also provided training to employees of the Prime Minister's Chancellery.

In 2023, the President of the Personal Data Protection Office and representatives of the Office actively participated in about 100 national and international events organised in Poland by the supervisory authority or other entities and in about 200 international and European events, including EDPB plenary meetings and subgroup meetings.

Challenges faced by the Personal Data Protection Office

The challenge for 2024 will also be to verify the provision of adequate protection for personal data processed with the use of clouds, applications, portals, shared systems or other IT solutions. These are increasingly widely used and - unfortunately - increasingly developed in disregard of the principles set out in the GDPR.

An important task is the involvement of the supervisory authority in legislative proceedings implementing European horizontal acts - especially from the so-called “digital package” - into national law.

The act that will require the most urgent work is the Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724). The act entered into force on 24 September 2023.

The second such relevant act is the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC), which has been in force since 17 February 2024.

***

As can be seen, the processing of personal data is a phenomenon that concerns almost all areas of life and affects all societal life. The President of the Personal Data Protection Office is aware that its work cannot be limited to expert activities, as the full record of its Report on its activities in 2023 shows.

Conclusions on the implementation of its tasks are drawn and analysed by the President of the Personal Data Protection Office on an ongoing basis, the effects of which are already visible. An important task of the President is to reach out to wider groups of citizens in order to effectively perform the tasks entrusted to it.

Let us just mention the Social Team of Experts to the President of the President of the Personal Protection Office, which was established in 2024 and which is supposed to facilitate the identification of relevant personal data issues and communicate the positions of the President of the Personal Data Protection Office.

The guides on the application of personal data law developed over the years need to be updated, which is already happening in the 2024 public consultation.

In 2024, the President of the Personal Data Protection Office has also started to work on simplifying the language used in the Office, in which legal issues are presented in an understandable and accessible way and good communication with citizens is ensured.