



OFFICE OF
THE DATA PROTECTION OMBUDSMAN

ANNUAL REPORT OF THE OFFICE OF THE DATA PROTECTION OMBUDSMAN 2023

ANNUAL REPORT
OF THE OFFICE OF THE DATA
PROTECTION OMBUDSMAN 2023



Contents

The Office of the Data Protection Ombudsman safeguards the rights and freedoms of individuals with regard to the processing of personal data	4
Data Protection Ombudsman Anu Talus: Data protection work in a changing digital environment.....	6
Deputy Data Protection Ombudsman Heljä-Tuulia Pihamaa: Consolidated positions, clarifications to the use of personal identity codes, and guidelines on children's data protection	9
Deputy Data Protection Ombudsman Annina Hautala: Data protection touches all parts of society	12
Office of the Data Protection Ombudsman's year 2023 in figures	14
Focus areas of data protection activities.....	16
Organisational reform, increasing number of cases and development of services	16
Number of personal data breach notifications keeps growing.....	19
Processing of cross-border cases	21
Support for controllers and DPOs	23
International transfers of data.....	24
Supervision and cooperation	26
Sanctions Board: Administrative fines for violations of data protection legislation	26
Auditing activities.....	28
Personnel and finances	29
Matters instituted and processed in 2021–2023	30

The Office of the Data Protection Ombudsman safeguards the rights and freedoms of individuals with regard to the processing of personal data

The Office of the Data Protection Ombudsman is an autonomous and independent authority that supervises compliance with data protection legislation and other statutes governing the processing of personal data.

The Office of the Data Protection Ombudsman promotes awareness of the rights, duties and opportunities related to the processing of personal data. The duties of the Office of the Data Protection Ombudsman include conducting investigations and inspections, issuing statements on legislative and administrative reforms and imposing sanctions

for violations of the General Data Protection Regulation (GDPR). The Data Protection Ombudsman cooperates with the data protection authorities of other countries and represents Finland on the European Data Protection Board.

In 2023, Anu Talus served as Data Protection Ombudsman, with Heljä-Tuulia Pihamaa and Annina Hautala as Deputy Data Protection Ombudsmen. The Data Protection Ombudsman and her deputies are independent in the performance of their duties. They are appointed for a five-year term by the government.

Societal objectives of the Office of the Data Protection Ombudsman

- We promote and safeguard the opportunities of people, companies and communities in a digitalising society.
- Our European cooperation is a resource for Finnish data protection.
- We safeguard the implementation of data protection in administrative reform and digitalisation projects.
- We ensure that potential data protection impact is taken comprehensively into account in law drafting.

Vision

The Office of the Data Protection Ombudsman is an active proponent for responsibility in the digital environment



Data Protection Ombudsman Anu Talus: Data protection work in a changing digital environment

The past year was eventful: the digital operating environment is constantly changing, the organisation of the Office of the Data Protection Ombudsman has evolved, and the supervisory authorities issued several significant decisions that shape the digital market.

The General Data Protection Regulation celebrated its 5th anniversary last year. Over the past five years, the importance of the digital operating environment has increased further and the amount of regulation has multiplied. My election as Chair of the European Data Protection Board (EDPB) in May 2023 came at a time when many of the provisions of the Commission's digital and data regulations were either finalised in Brussels or implemented domestically.

New digital regulation will be built on the GDPR. Although the starting point may seem simple, there is a lot of overlapping regulation. Therefore, cooperation between authorities is all the more important. In addition to the new digital projects, the Commission presented its proposal for a provision supplementing the GDPR with the aim of streamlining cooperation between authorities in cross-border matters between EU Member States.

The year was also marked by new legislative projects nationally. The Data Protection Act was amended by adding a provision on so-called inactivity complaints. If the Office of the Data Protection Ombudsman does not notify about the progress of the complaint within three months, the person may appeal to the Administrative Court. At the same time, a provision was introduced into the Data Protection Act that enables the referendaries of the Office to resolve cases on which there already is established policy. The amendments entered into force at the beginning of 2024.

The number of new cases, which had remained stable for three years, started to rise again sharply. Over 2,000 more cases were initiated during the year than in the previous year, a total of 13,179 cases. Almost as many cases were resolved as initiated. This is a testament to the tireless work of our specialists. However, it is clear that as tasks increase due to new legislation and matters become more complex and difficult, additional resources will be needed to carry out statutory tasks.

The organisational structure of the Office of the Data Protection Ombudsman was renewed in April 2023. Changes were made, for example, to units and the responsibilities of ombudsmen. New supervisor positions and expert positions requiring long experience were also created. In an expert organisation, it is important to recognise the importance of deepening and broadening expertise.

The Office also quite successfully introduced a new case management system. The new system improves work efficiency, promotes knowledge-based management and creates new kinds of opportunities to develop operations based on more accurate statistical data than before.

In addition to adopting new legislation and developing the organisation, day-to-day data protection and supervision work was at the core of the operations. For example, we issued 44 legislative opinions during the past year. In the election year, the Government's legislative work began in earnest in the autumn.

A number of important decisions were also made during the year. In some decisions, an administrative fine was imposed on the controller, while in others, the controller was ordered to rectify its actions. During the year, administrative fines were imposed on three controllers. In two cases, a fine was imposed for non-compliance with a previous order of the Data Protection Ombudsman.

The sanctions board of the Office of the Data Protection Ombudsman also dealt with other important matters, for example, a so-called urgent procedure was used in a decision concerning taxi service Yango that temporarily banned data transfers to Russia. Processing of the case has since continued in cooperation with the Dutch and Norwegian supervisory authorities.

During the year, the Administrative Court and the Supreme Administrative Court issued several decisions concerning data protection, which confirmed the Data Protection Ombudsman's policy on the application of the GDPR.

European cooperation has become a part of the authority's statutory tasks since the GDPR became applicable. The most significant EU-level decision of the year is probably the Commission's so-called adequacy decision on the level of data protection in the United States. The EDPB issued a positive opinion to the European Commission on the new EU-US data protection framework, although it expressed some concerns about the whole.

The Office of the Data Protection Ombudsman has also contributed to the dispute resolution decisions of the European Data Protection Board. Last year, following the EDPB's decision, a fine of 1.2 billion euros was imposed on Meta for data transfers to the United States, and a fine of 345 million euros on TikTok for breaches of children's privacy. In addition, the EDPB adopted an urgent binding decision against Meta, in which it considered that Meta had processed personal data for the purpose of targeting advertising to individuals without an appropriate legal basis.


March also saw the launch of the EDPB's second coordinated enforcement action, which, on the initiative of the Office of the Data Protection Ombudsman, focused on the designation and position of Data Protection Officers in organisations. In the spring, the EDPB published a guide for SMEs, the Finnish translation of which will be available during 2024. The position of SMEs will also be on the agenda of the EDPB's next strategy, which was adopted in spring 2024. The *GDPR4CHLDRN – Ensuring data protection in hobbies project*, which promotes children's data

protection and is funded by the Commission, proceeded in cooperation with TIEKE Finnish Information Society Development Centre, coordinated by the Office of the Data Protection Ombudsman.

The discussion about artificial intelligence continued intensively over the past year and will continue to be highly relevant in 2024. The EDPB set up a working group on ChatGPT, and decisions by national supervisory authorities on artificial intelligence can be expected during 2024. A political agreement has been reached on the Artificial Intelligence Act, and national supervisory authorities will play an important role in its application, regardless of which authority supervises the AI Act.



Anu Talus
Data Protection Ombudsman



Deputy Data Protection Ombudsman
Heljä-Tuulia Pihamaa:

Consolidated positions, clarifications to the use of personal identity codes, and guidelines on children's data protection

The reform of the Office of the Data Protection Ombudsman's organisation entailed changes to the Office's units and the responsibilities of the Ombudsmen. At the beginning of April 2023, I changed from heading the public-sector customer service team to managing the private-sector guidance and supervision unit.

In the private sector, financial sector matters were the largest group in terms of matters instituted with the Office. We were kept particularly busy with personal data breach notifications, matters involving the right of access, requests for the erasure of data, and cases related to payment default entries.

An administrative fine was imposed in the financial sector in 2023 for unfounded payment default entries made on the basis of judgments in civil cases. The company had not erased the data from its credit information register despite an order issued in 2021.

One of the key positions adopted by the Data Protection Ombudsman in the private sector involved the lawfulness of purchase data storage times in the retail sector. The storage of purchase data for the whole duration of loyalty programme membership, in practice often for decades, cannot be considered to comply with data protection legislation. If the processing of personal data is an essential part of a company's business, it must strictly observe the principles of processing of personal data, such as data minimisation and determining storage periods. This will only increase in importance in our data-driven economy and will be reflected in the Office of the Data Protection Ombudsman's decisions going forward.

As a rule, the Office of the Data Protection Ombudsman's decisions were upheld by the administrative courts. In September, the Supreme Administrative Court issued its decision on the administrative fine imposed on Posti in the spring of 2020. It was the first Sanctions Board decision to be taken to the Supreme Administrative Court. The Court enforced the administrative fine, which had been imposed for shortcomings in informing people who had submitted a notification of change of address. It is noteworthy that, in its decision, the Supreme Administrative Court confirmed that the supervisory authority had been within its rights in imposing the administrative fine before exercising its other corrective powers, such as issuing an order or reprimand.

In December, the Administrative Court of Eastern Finland issued a decision in the "log data case". The decision was based on a preliminary ruling issued by the European Court of Justice. In the main, the Administrative Court decision upheld the Deputy Data Protection Ombudsman's position and thus the Office of the Data Protection Ombudsman's established interpretation of the disclosure of user log data. According to the Administrative Court decision, a bank is not obliged to disclose information on the bank's employees who had accessed the customer's data. However, the bank is required to disclose the precise times when the customer data was accessed from the user logs. The decision has been appealed, so we will wait for the Supreme Administrative Court's decision on the matter.

The processing of personal identity codes was clarified by law. In December, Parliament approved amendments to the Data Protection Act and the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security. The provisions on the processing of personal identity codes were also clarified in this connection. The amendment is intended to highlight the original purpose of the personal identity code as a means of individualisation, that is, telling people apart from each other. The law was clarified with an amendment that entered into force at the beginning of 2024 and states that a person may not be identified with their personal identity code alone or with a combination of their name and personal identity code. The use of personal identity codes for identifying individuals in addition to their original purpose of telling specific individuals apart has become a problem. It is to be hoped that the amendment will clarify practices on the ground.

In June, the Supreme Administrative Court issued a decision on processing the personal identity codes of children. The Supreme Administrative Court upheld the Deputy Data Protection Ombudsman's position, according to which regularly collecting the personal identity codes of the children of all tenants and everyone applying for a rental home by property managers and lessors is not necessary under the General Data Protection Regulation. Even though the law permits the processing of personal identity codes in renting, such processing must always be necessary.

Children's data protection was the focus of our operations in 2023, which was reflected in the continuation of the *GDPR4CHLDRN – Ensuring data protection in hobbies* project, among other things. The project is a two-year EU-funded project by the Office of the Data Protection Ombudsman and TIEKE Finnish Information Society Development Centre intended to improve the practical data protection knowledge of children and young people aged 13–17, their parents, and associations that organise hobby activities. Among other things, the project will produce a "digital toolkit" to help associations resolve issues related to compliance with data protection legislation. The project will conclude in late 2024.



Heljä-Tuulia Pihamaa
Deputy Data Protection Ombudsman



Deputy Data Protection Ombudsman
Annina Hautala:

Data protection touches all parts of society

The year 2023 was my first full year as Deputy Data Protection Ombudsman. It was another interesting and busy year on the data protection front. As I say in the title of this piece, data protection cross-cuts society and is important to every one of us. Its significance is perhaps even greater in public administration, since people often do not have a say in whether public authorities process their data or not. Special categories of personal data, such as health information, are also widely processed by the public administration.

The public-sector guidance and supervision unit was placed under my responsibility in the Office of the Data Protection Ombudsman's organisational reform in April 2023. The organisational reform merged the data protection guidance and enforcement of the security and judicial administration sector with that of other sectors of the public administration. With this change, we are able to build a more comprehensive picture of the state of data protection in the

public administration and of where to focus enforcement. The aim is to allocate our resources to the enforcement and guidance actions that have the most impact and thus ensure the realisation of data protection for everyone as required by law.

As in previous years, social welfare and health care was the largest sector in terms of matters instituted with the Office of the Data Protection Ombudsman in 2023. The most common matters instituted with the Office, both in social welfare and healthcare and in other public sectors, were personal data breach notifications and matters involving the exercise of the rights of the data subject, such as requests concerning the right of access and right to erasure. The launch of the new wellbeing services counties and the amendment to the Act on the Processing of Client Data in Healthcare and Social Welfare, which entered into force at the start of 2024, were also reflected in our work in the social welfare and healthcare sector.

In addition to the organisational reform, the Office of the Data Protection Ombudsman developed its practices and processes in order to improve the efficiency of its operations. For example, the processing of matters involving social welfare and healthcare was improved by introducing a screening procedure for cases involving the rights of individuals. We also allocated more human resources to enforcement work in the sector.

The year was also full of reform in the education and early childhood education sector. The Office of the Data Protection Ombudsman issued several reminders about data protection to the parties responsible for the preparation and implementation of the reforms. The subjects of the reforms included the processing of personal data in basic education and the organisation of student welfare. Several legislative projects related to the work of the security authorities were also initiated in 2023, and the Office of the Data Protection Ombudsman supported the preparation of these projects from the perspective of data protection.

Our enforcement activities in 2023 also included planned audits of controllers. The goal of such audits is to identify development needs before risks involving personal data are realised. At the same time, they serve to increase the organisations' knowledge and awareness of data protection. Our Office was also the subject of an inspection as part of the evaluation of Schengen states' compliance with EU law. Last year, it was Finland's turn for this regular inspection.

The considerable number of "snooping" cases found by our enforcement measures and through pre-trial investigation authorities' and prosecutors'

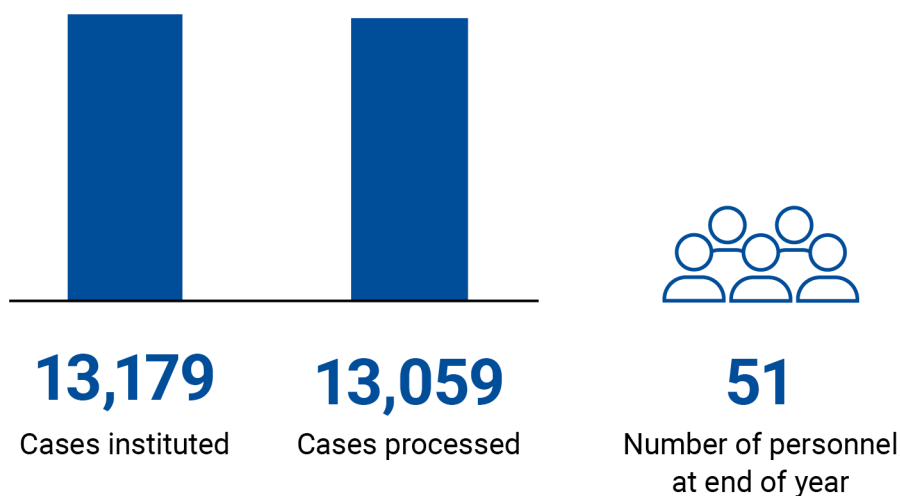
requests for statements is noteworthy. Some of these cases have been extensive and protracted. The pre-trial investigation authority or prosecutor is required to request a statement from the Data Protection Ombudsman on matters involving a data protection offence, secrecy offence, unlawful access to an information system or violation of the secrecy of communications. The number of such requests increased from 37 in 2022 to 54 in 2023.

Due to the above-mentioned observations, the monitoring of processing in the operations of controllers was adopted as a special theme for the 2024 audit plan. I cannot overstate the importance of the active self-monitoring of processing by the controller in addition to looking after the security of data files and information systems, access rights management, and instructing users.



Annina Hautala
Deputy Data Protection Ombudsman

Office of the Data Protection Ombudsman's year 2023 in figures



In 2023, the Office of the Data Protection Ombudsman issued

- 3** decisions imposing administrative fines for data protection violations
- 41** reprimands for processing measures that violated data protection legislation
- 20** orders to bring personal data processing measures into compliance with the GDPR
- 6** orders to fulfil the rights of the data subject
- 2** orders to notify data subjects about a personal data breach



6,894

Personal data
breach notifications



11

Inspections
carried out



2,856

Calls answered by
the telephone service



44

Statements on
legislative projects



54

Statements to
prosecutors and pre-trial
investigation authorities



6

Lead supervisory
authority in
cross-border
cases

147

Supervisory authority
concerned in
cross-border
cases

Organisational reform, increasing number of cases and development of services

Changes were made to the Office's units and the responsibilities of the Ombudsmen. The new organisation consists of a private-sector guidance and supervision unit, public-sector guidance and supervision unit, administrative unit, and management support and core services unit. The Office's administrative, information management and registry services have

The Deputy Data Protection Ombudsmen are responsible for the monitoring of the private and public sectors. The Data Protection Ombudsman's responsibilities include the supervisory authority's general policies, European cross-border cooperation, and liaising with the European Data Protection Board (EDPB).

```

graph TD
    DPO[Data Protection Ombudsman]
    DPO --- DPO_O[Data Protection Officer]
    DPO --- AM[Administrative Manager]
    DPO --- MSS[Management Support and Core Services]
    DPO --- GSPS[Guidance and supervision on private sector]
    DPO --- GSPS_P[Guidance and supervision on public sector]
    DPO -.-> DDO[Deputy Data Protection Ombudsman]
    DDO -.-> DDO2[Deputy Data Protection Ombudsman]
    DDO2 -.-> SB[Sanctions Board]
    EB[Expert Board]
    AM --- Admin[Administration]
    Admin -.-> MSS
    MSS -.-> GSPS
    GSPS -.-> GSPS_P
    GSPS_P --- DT[Development teams]
    style DT fill:#0056b3,color:#fff
  
```

The organizational chart of the Data Protection Commission (DPC) is structured as follows:

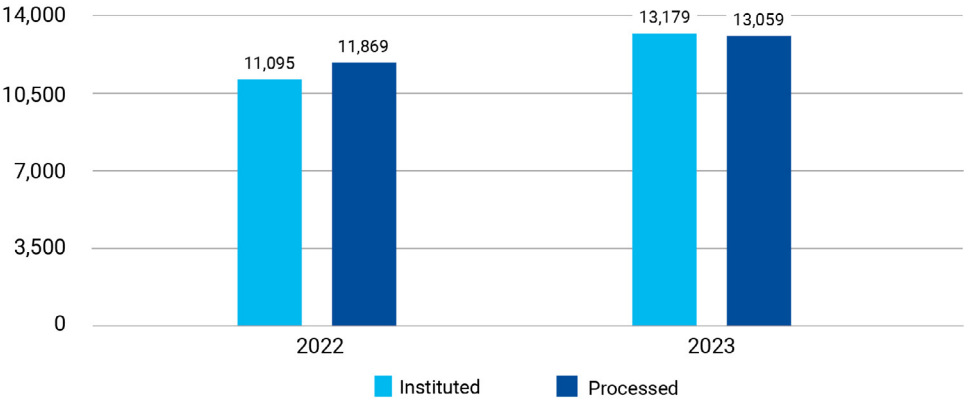
- Data Protection Ombudsman** (top level)
 - Data Protection Officer** (reports directly to the Ombudsman)
 - Administrative Manager** (reports directly to the Ombudsman)
 - Administration** (reports to the Administrative Manager)
 - Management Support and Core Services** (reports to Administration)
 - Management Support and Core Services** (reports directly to the Ombudsman)
 - Guidance and supervision on private sector** (reports to Management Support and Core Services)
 - Guidance and supervision on public sector** (reports to Management Support and Core Services)
- Deputy Data Protection Ombudsman** (reports to the Ombudsman)
 - Deputy Data Protection Ombudsman** (reports to the first Deputy)
 - Sanctions Board** (reports to the second Deputy)
- Expert Board** (advisory body, reports to the Ombudsman)
- Development teams** (support function, reports to the Guidance and supervision on public sector)

After fairly stable volumes in recent years, the number of cases instituted with the Office of the Data Protection Ombudsman grew clearly in 2023, with a total of 13,179 cases instituted with the Office. This was approximately 2,000 cases more than in the previous year. The number of cases resolved also increased, with 13,059 cases closed in 2023.

Personal data breach notifications were the most common type of cases instituted with the Office, accounting for 52 per cent of all cases instituted. The number of cross-border EU cases also grew.

The Office of the Data Protection Ombudsman has been systematically clearing its case backlog since 2020. At the end of 2023, there were approximately 880 unresolved cases instituted in 2018–2021 that had been pending for more than two years. Cross-border cases led by the supervisory authority of another EEA state constitute a significant part of these older unresolved cases.

Matters instituted and processed from 2022 to 2023



Flow of operations improved through system updates

The improvement of information management has been defined as the Office's key goal for the next few years. In the autumn of 2023, the Office adopted a joint case management system for agencies in the judicial administration, made a comprehensive overhaul of the organisation's information management guidelines, and developed the Office's information management model. The new case management system makes the processing of cases more efficient and improves knowledge-based management.

At the end of the year, the Office of the Data Protection Ombudsman adopted a secure form service provided by the Government ICT Centre Valtori. Organisations can use the forms to file personal data breach notifications, declare the contact details of their data protection officers, and request prior consultations. Private individuals can use the forms to request an order regarding the exercise of their data protection rights or report faults they have noticed in the processing of personal data. Sent forms can be saved as PDF files for the customer's own use. With the adoption of the secure form service, the forms can now be used to send confidential and sensitive information to the Office of the Data Protection Ombudsman.

The Office's internal procedures were also developed in order to improve the efficiency of case processing. Screening procedures in matters concerning the rights of the data subject and the processing of personal data breach notifications were established and refined.

The personal data breach notification screening procedure adopted in 2022 has made the processing of the notifications significantly more efficient. The screening looks at questions such as whether the case needs to be taken further with the controller and whether the breach requires official action.

The screening of cases concerning the rights of the data subject continued in matters related to the social welfare and healthcare sector. The Office is considering applying the model to other sectors as well.

In December 2023, Parliament passed amendments to the Data Protection Act and the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security to bring them into line with EU data protection legislation. From the beginning of 2024, the Office of the Data Protection Ombudsman is required to resolve a complaint or give the complainant an estimate of when a decision will be issued within three months of the matter's institution. People can appeal to the Administrative Court if the Data Protection Ombudsman does not issue a decision or provide an estimate of the processing time within this time limit.


Number of personal data breach notifications keeps growing

Personal data breach notifications constitute the largest single category of cases instituted with the Office of the Data Protection Ombudsman. If a personal data breach can cause a risk to the people affected by it, the Office of the Data Protection Ombudsman must be notified. If necessary, the Office can order an organisation to notify the person concerned of the breach.

A total of 6,894 data breach notifications were filed with the Office during the year, representing an increase of more than 1,400 from the previous year. The numbers of reported data breaches have increased annually and constituted as much as 52 per cent of cases instituted. This number is in line with our European reference countries.

The growth is probably partly due to the general increase in digitalisation and advancements in information technology. Public awareness of the notification duty concerning personal data breaches has also increased steadily. The most notifications are received from regulated sectors, such as social welfare and health care, the financial sector and the telecommunications sector.

In the autumn, the Office of the Data Protection Ombudsman reminded organisations that they should assess the seriousness of personal data breaches from the points of view of the data subjects concerned. Complying with the GDPR's requirements for handling personal data breaches requires organisations to assess the seriousness of the consequences to the data subjects instead of the consequences to the controller. The controller should also consider carefully what measures it could take to mitigate the negative consequences to individuals.



The Office of the Data Protection Ombudsman received 6,894 personal data breach notifications in 2023.

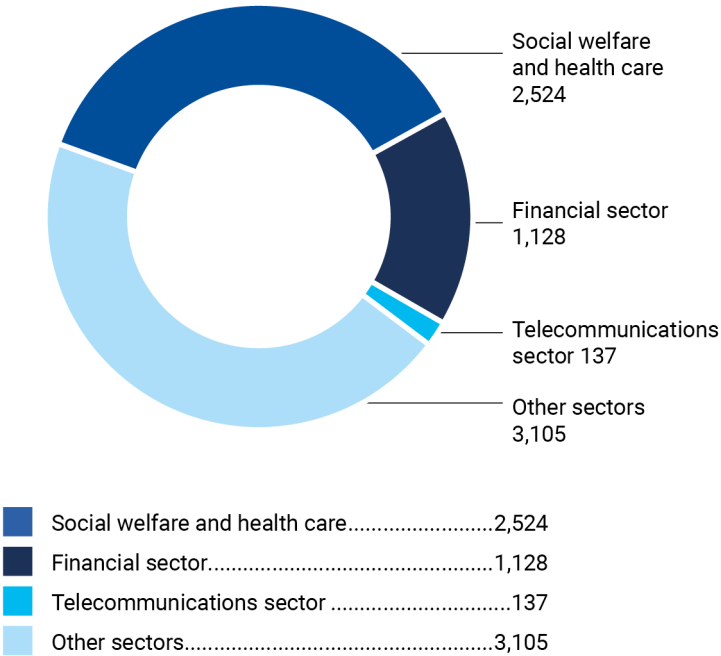
If a controller submits a preliminary notification of a personal data breach to the Office, it should remember to supplement the notification later on its own initiative. Preliminary notifications which organisations have not supplemented on their own initiative cause a great amount of investigation work to the Office. A personal data breach notification must be made without undue delay and no later than in 72 hours of detecting the breach. If the notification is delayed, a justified explanation of the reason must be made to the Office.

Many personal data breaches could be prevented with adequate technical safeguards, appropriate organisational procedures and data protection expertise. Old systems that have not been updated, and especially shortcomings in data security, expose organisations to personal data breaches. System vulnerabilities are also being exploited more quickly than before. Such breaches often also concern personal data stored in the system.

Office 365 data leaks remain common. They are often caused by human error when someone opens a link in an email and enters their password or credentials. The most serious personal data breaches involving email follow the storage of material containing large amounts of personal data, such as personal identity codes, job applications or sick leave certificates, in an email inbox.

The Office of the Data Protection Ombudsman made some improvements in 2023 to the way in which personal data breach notifications are submitted. The adoption of Valtori’s secure form service in the autumn lets organisations save submitted forms directly in the service. Saving the notification helps with documenting data breaches and demonstrating compliance with the organisation’s accountability obligation.

Personal data breach notifications
instituted by sector, 2023



Processing of cross-border cases

Cross-border processing' means the processing of personal data

- performed in offices located in more than one Member State or by a controller or processor established in more than one Member State; or
- performed in the EU in the controller's or processor's only office, but the processing has a significant impact on data subjects in more than one Member State.

When the processing of personal data crosses borders, the data protection authorities of the European Economic Area (EEA) monitor the processing of personal data in cooperation. A 'lead supervisory authority' is appointed for the case and works together with the other supervisory authorities participating in the processing of the matter. The purpose of the cooperation procedure is to achieve a binding common decision by the supervisory authorities, as well as to ensure the consistent application of the GDPR across the EEA. The European Data Protection Board has a register of joint decisions taken by data protection authorities on its website.

During the year, the data protection authorities considered cases involving major social media companies in cross-border cooperation. Many large social media companies have their European headquarters in Ireland, so the Irish data protection authority is the lead supervisory authority in these cases. All participating data protection authorities from the EEA, including the Office of the Data Protection Ombudsman, are involved in the decision-making.

In 2023, the Office of the Data Protection Ombudsman was designated as the lead supervisory authority in 6 cases and as a supervisory authority concerned in 147 cases.

In April, the European Data Protection Board issued a binding dispute-resolution decision concerning the lawfulness of Meta's transfers of data to the United States in the Facebook service. The EEA data protection authorities that participated in the case, including the Office of the Data Protection Ombudsman, concurred with Ireland's views on Meta's violations and found that Meta's transfers of data had been in violation of the GDPR from July 2020. Following the EDPB's decision, the Irish data protection authority imposed an administrative fine of EUR 1.2 billion on Meta and ordered Meta to suspend the transfer of European users' personal data to the US. Meta was also ordered to bring the transfers of data into compliance with the GDPR within six months.

In August, the EDPB issued a decision on the processing of children's personal data in TikTok, following a dispute resolution procedure. Based

on the binding decision, Ireland imposed an administrative fine of EUR 345 million on TikTok for several violations in the processing of children's personal data and ordered the company to stop using misleading formatting solutions that violate the GDPR. Among other things, the violations concerned the application's default settings that made children's accounts public by default.

Based on a decision made by the EDPB in October, Ireland ordered Meta to stop the processing of personal data for behaviour-based targeted advertising based on the controller's legitimate interest or the performance of an agreement. The decision was made with the urgent procedure after the Norwegian data protection authority had asked the EDPB to decide on EEA-wide action concerning Meta.

In September 2023, the Finnish, Dutch and Norwegian data protection authorities agreed on the next steps in investigating the Yango taxi service's (Yandex LLC and Ridetech International B.V.) transfers of data to Russia. The lawfulness of Yango's actions will be assessed and decided in a cross-border procedure, in which the Netherlands serves as the lead supervisory authority and cooperates with the Finnish and Norwegian data protection authorities. The Office of the Data Protection Ombudsman does not have the power to make a final decision concerning Yango, which can only be issued by the Dutch data protection authority.

In 2023, the Office of the Data Protection Ombudsman issued one cross-border decision within the EU as a lead supervisory authority. The accommodation service Forenom Oy was reprimanded for inadequate safeguards and ordered to shorten the storage period of customer data. An attacker had used an SQL injection to obtain access to Forenom's customer self-service portal and ERP system through an API vulnerability, giving the attacker access to a database containing the data of tens of thousands of customers.

The Office of the Data Protection Ombudsman issued a total of two objections to draft decisions by leading supervisory authorities in cross-border cases during the year.

In April, the Norwegian data protection authority imposed an administrative fine of NOK 10 million (approximately EUR 900,000) to the SATS gym chain for a variety of data protection violations. In particular, the violations concerned the fulfilment of the rights of the data subject, informing customers, and the lack of a basis for processing personal data. The gym chain operates in Norway, Finland, Sweden and Denmark, so the Office of the Data Protection Ombudsman participated in the investigation.

During the year, the Office submitted two objections to draft decisions made by lead supervisory authorities. The Office also influenced the contents of draft decisions in several cases.

In July, the European Commission issued a legislative proposal for the harmonisation of administrative procedures in cross-border cases within the EU. The new regulation aims to simplify and expedite the processing of cross-border cases and to promote cooperation between supervisory authorities from the first stages of the process. The Commission issued the legislative proposal on the basis of an initiative introduced by the EDPB in the autumn of 2022. In September, the EDPB and the European Data Protection Supervisor issued a joint statement calling for the rapid adoption of the regulation. On the national level, the Office of the Data Protection Ombudsman also gave its opinion on the Commission's proposal to the Ministry of Justice and to Parliament.

Support for controllers and DPOs

Study of the position and appointment of DPOs

Together with 25 European data protection authorities, the Office of the Data Protection Ombudsman participated in a joint measure coordinated by the EDPB for investigating the designation and status of data protection officers in organisations in a variety of industries and sectors. DPOs were chosen as the subject of the measure on the Office of the Data Protection Ombudsman's initiative.

The measure was launched with a joint survey for organisations, which the Office of the Data Protection Ombudsman sent to 50 Finnish organisations in May 2023. Seven government agencies, 20 municipalities, six wellbeing services counties, six financial service providers, three telecommunications operators and eight platform service providers were selected for the study. The survey was taken by more than 17,000 organisations across Europe.

The EDPB published a report of the study in January 2024. Most of the respondents felt that they had clearly defined duties and the competence required for their work, but many DPOs still face challenges in their duties. The report describes identified development needs and issues recommendations for reinforcing the status of DPOs. The challenges reported were related to matters such as a lack of resources, the independence of the DPO, and reporting to senior management. The survey's national results are available in an annex to the report.

The supervisory authorities will decide on follow-up measures required at the national level based on the study's findings. These follow-up measures will be implemented in Finland in 2024.

GDPR4CHLDRN project improves data protection awareness in hobby activities for children and young people

The Office of the Data Protection Ombudsman's and TIEKE Finnish Information Society Development Centre's two-year, EU-funded project *GDPR4CHLDRN – Ensuring data protection in hobbies* continued in 2023. The project is funded by the Citizens, Equality, Rights and Values EU programme. The project's stakeholder partners are the Guides and Scouts of Finland, the Football Association of Finland, and the Finnish Olympic Committee.

The project is aimed at improving the data protection competence of children and young people aged 13–17, their parents and clubs and associations that organise hobby and leisure activities for them. The goal is that, in future, clubs and associations will be able to use the materials produced in the project to resolve issues related to compliance with data protection legislation in their activities.

The project will create a digital toolkit for associations, containing practical materials for various audiences, such as guides, checklists, and tests for charting one's knowledge. These materials promote awareness of data protection and the processing of personal data among children and young people and their parents. Development of the materials continued with the different target groups during the year. The project published 5 newsletters and 14 expert articles and participated in the Media Literacy Week.

In 2024, the project will continue with piloting of the materials. Training and webinars about data protection were held for association employees in the spring, and the toolkit will be rolled out in stages over the summer. The project will conclude in the autumn of 2024.

International transfers of data

When personal data is transferred outside the European Economic Area or to an international organisation, the level of protection for personal data may not correspond to the requirements of the EU General Data Protection Regulation. For this reason, a number of bases for transferring personal data have been specified in the GDPR, which can be used to transfer personal data out of the EEA. The Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security also has provisions on international transfers of data. Before starting the transfer of personal data, the controller or processor must verify on a case-by-case basis whether an adequate level of data protection is guaranteed for the personal data being transferred.

The transfer of personal data to the United States was made easier in July 2023, when the European Commission adopted an adequacy decision on the level of data protection in the United States. The new Data Privacy Framework between the EU and the United States replaced the earlier Privacy Shield arrangement, which was nullified by the Court of Justice of the EU's Schrems II judgment (C-311/18) in 2020.

In March, the EDPB issued its statement on the draft adequacy decision, recognising major improvements but also raising certain concerns. The Office of the Data Protection Ombudsman actively influenced the contents of the statement. The EDPB statement plays a key role in the Commission's evaluation of the adequacy of data protection in a third country.

The transfer of personal data to the United States was made easier in July 2023, when the European Commission adopted an adequacy decision on the level of data protection in the United States.

An adequacy decision permits the transfer of data without additional safeguards from the EU and EEA to US companies that are committed to the Data Privacy Framework's requirements. Data can only be transferred to certified organisations listed in the Data Privacy Framework list maintained by the US Department of Commerce. Transfers of data between public-sector organisations cannot be based on an adequacy decision.

The EDPB has drawn up info materials for controllers about the EU–U.S. Data Privacy Framework. In late 2023, the Office of the Data Protection Ombudsman published an online FAQ of the adequacy decision’s practical impact.

In January 2023, the EDPB published a report of the first joint measure by the European data protection authorities, which examined the use of cloud services in the public sector. The Office of the Data Protection Ombudsman contributed to the report, which issued recommendations concerning the use of cloud-based products and services to public-sector organisations. The annex to the report also described measures related to cloud services taken by data protection authorities to date.

The EDPB’s binding decision of April 2023, referred to above, commented on the lawfulness of Meta’s transfers of data to the United States. The decision found that all transfers of data from July 2020 had violated the GDPR, since the company had continued transferring personal data to the United States after the CJEU’s Schrems II judgment (C-311/18) of July 2020 without appropriate safeguards.

The guidelines on international transfers of data were supplemented in 2023. In the spring, the EDPB published the final version of the guideline on the interplay between the application of Article 3 of the GDPR and the provisions on international transfers of data. The guideline clarifies the definition of international transfers and helps organisations recognise them.

The EDPB also published a final guideline on certification as a tool for transfers. In June, the EDPB published recommendations on Controller Binding Corporate Rules (BCR-C). In the summer of 2023, the Office of the Data Protection Ombudsman also issued a decision on an administrative arrangement between the Finnish Patent and Registration Office and the US Public Companies Accounting Oversight Board.

Supervision and cooperation

Sanctions Board: Administrative fines for violations of data protection legislation

The sanctions board of the Office of the Data Protection Ombudsman is tasked with matters involving the imposition of administrative fines under the General Data Protection Regulation on controllers or processors. The Sanctions Board is made up of the Data Protection Ombudsman and two Deputy Data Protection Ombudsmen. The Board is chaired by the Data Protection Ombudsman. In 2020–2023, the Sanctions Board has imposed a total of 20 administrative fines for violations of the GDPR.

Administrative fines are one of the corrective powers available to the Office of the Data Protection Ombudsman. An administrative fine must be dissuasive, effective and proportionate. An administrative fine can be imposed in addition or instead of other corrective measures and is limited to a maximum of 4% of the

company's turnover or EUR 20 million. At present, administrative fines cannot be imposed on public organisations, such as the central government and state-owned companies, municipalities or parishes. Extending the application of administrative fines to the public sector has been recorded as a goal in the current Government Programme. Administrative fines can already be imposed on public-sector entities in the other Nordic countries.

Administrative fines were imposed on three organisations in 2023. Fines were imposed for non-compliance with the Data Protection Ombudsman's prior order, violations concerning recorded phone calls, and shortcomings in fulfilling the data subject's right of access. The administrative fines ranged from 1,600 to 440,000 euros.

In 2023, the Sanctions Board imposed administrative fines on three organisations for violations of data protection legislation.

- Suomen Asiakastieto Oy was ordered to pay an administrative fine of 440,000 euros, as the company had not erased unfounded payment default entries made in its credit information register due to faulty practices despite being ordered to by the Data Protection Ombudsman. Data based on judgments in civil matters should not have been saved as payment default entries. In November 2021, the Data Protection Ombudsman had ordered the company to correct its practices regarding the registration of payment default entries and to erase all incorrect payment default entries made due to those practices.
- Suomen Yritysrekisteri, a company maintaining a corporate directory, was ordered to pay an administrative fine of 23,000 euros because it had not delivered phone call recordings to people who had requested them according to data protection provisions. The compilations of call recordings delivered by the company did not meet the GDPR's requirements on copies that would correspond to the contents of the original call. In addition, the company had ignored the Deputy Data Protection Ombudsman's earlier order to bring their operations into compliance with the law. The company should have offered another method of obtaining the recordings in addition to listening to them.
- The Sanctions Board ordered a psychotherapy provider to pay an administrative fine of 1,600 euros due to shortcomings in fulfilling the data subject's right of access. A customer of the psychotherapy provider had made several requests to access their data between 2017 and 2019. The psychotherapy company had not provided the data to the customer or given a reason for why it was unable to deliver the data within the time limits specified by the GDPR.

The Office of the Data Protection Ombudsman's Sanctions Board also processes matters concerning the prohibition of processing. In the autumn of 2023, the Sanctions Board processed the interim suspension order issued to Yandex LLC

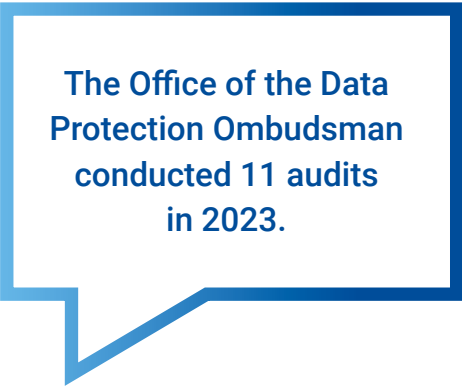
and Ridetech International B.V. and evaluated the possibility of transferring the case to the EDPB. In this case, the Board found that a cross-border procedure with the Netherlands and Norway was the best option for resolving the matter.

Auditing activities

The audits carried out by the Office of the Data Protection Ombudsman are based on identified risks related to the processing of personal data and on the supervision and auditing obligations arising from EU law and national special legislation.

The Office of the Data Protection Ombudsman had drawn up an advance plan for audits to be carried out in 2023. Restrictions of the data subject's right of access and the possibilities of data subjects to monitor the processing of their own personal data were special themes in the audits for this year. The audits thus focused on security authorities which limit the right of access, such as for the purpose of safeguarding the integrity of investigations.

The Office conducted 11 audits according to the audit plan in 2023. The audits did not give cause to exercise the Ombudsman's corrective powers, but guidance and recommendations were given to controllers as a result of observations made in the inspections.



**The Office of the Data
Protection Ombudsman
conducted 11 audits
in 2023.**

The European Commission conducted an evaluation of the Schengen Information System in the summer of 2023. The implementation of the Schengen acquis in the Member States is monitored with the Schengen evaluation and monitoring mechanism. The evaluation is carried out every four years, and as the national supervisory authority, the Office of the Data Protection Ombudsman was one of the authorities evaluated.

Personnel and finances

– updates to organisation structure

There were no changes in the number of personnel employed by the Office of the Data Protection Ombudsman from 2022. A total of 51 people were employed by the Office at the end of the year.

The customer service teams that had operated in the Office were discontinued, and the new units started their work on 24 April 2023. These units are the private-sector guidance and supervision unit, public-sector guidance and supervision unit, administrative unit and management support and core services unit. The management support and core services unit is led by the Data Protection Ombudsman, the private-sector unit and public-sector units by the Deputy Ombudsmen, and the administrative unit by the Head of Administration.

New team manager's posts were introduced in the private-sector and public-sector units in connection with the restructuring. The team managers supervise the work of the Office's inspectors and legal experts.

The duties of the Office of the Data Protection Ombudsman are expected to increase in the coming years, for example due to new tasks arising from the EU's digital and data legislation.

Human resources*	2021	2022	2023
Number of personnel at the end of the year	55	54	54
Person years	49.1	51.9	52.7
Absences due to illness, day(s) per person years	10.4	13.2	5.6
Average age	40.3	39.3	42.1
Education index	6.2	6.4	6.4

* The figures include the personnel of the Office of the Data Protection Ombudsman and the Function of the Intelligence Oversight Ombudsman (3 persons). The Function of Intelligence Oversight Ombudsman shares administrative functions with the Office of the Data Protection Ombudsman.

Finances of the Office of the Data Protection Ombudsman	Realisation 2021	Realisation 2022	Target 2023	Realisation 2023
Use of the operating expenses appropriation, €1,000	3,912	4,041	5,343	4,324
Total costs, €1,000	4,351	4,450	-	4,730

Matters instituted and processed in 2021–2023

The table below presents how many cases have been instituted and how many cases have been resolved by the Office of the Data Protection Ombudsman in 2021–2023. The statistics have been compiled from

the Office's case management system at the end of the year in question. The Office adopted a new case management system in October 2023.

	2021		2022		2023	
	Instituted	Resolved	Instituted	Resolved	Instituted	Resolved
Tasks in accordance with the GDPR and the Data Protection Law Enforcement Directive						
Prior consultation (high risk)	88	22	71	249	23	25
Statements	392	398	408	417	287	301
Codes of Conduct	1	2	0	1	0	2
Transfers of personal data	54	25	26	18	3	18
EU and international cooperation	811	760	1,018	1,016	1,362	1,297
Rights of the data subject	943	984	834	950	838	994
Supervision	1,139	1,145	1,063	1,069	1,268	1,197
Personal data breaches	4,786	5,056	5,446	5,663	6,894	6,487
Guidance and advice	1,650	2,037	1,176	1,441	1,318	1,592
Data Protection Officers	323	323	255	269	267	260
Board of Experts	3	4	2	2	2	2
General, financial and human resource issues	630	630	796	774	917	884
Total	10,820	11,386	11,095	11,869	13,179	13,059



OFFICE OF
THE DATA PROTECTION OMBUDSMAN

P. O. Box 800, FI-00531 Helsinki, Finland
tel. +358 29 566 6700 (switchboard)
tietosuoja@om.fi
www.tietosuoja.fi