OFFICE OF
THE DATA PROTECTION OMBUDSMAN

ANNUAL REPORT
OF THE OFFICE OF THE DATA PROTECTION OMBUDSMAN OF FINLAND 2024

ANNUAL REPORT

OF THE OFFICE OF THE DATA PROTECTION OMBUDSMAN OF FINLAND 2024

Contents

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 (EDPB).

In 2024, Anu Talus served as the 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. The Data Protection Ombudsman is responsible for the general guidelines of the supervisory authority, cross-border collaboration in Europe and tasks related to the European Data Protection Board. The Deputy Data Protection Ombudsmen are responsible for supervision of the private and public sector.

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.
- We safeguard everyone's right to personal data protection and the citizens' trust in the transparency of personal data processing.
- We ensure that data protection and any effects to it are taken into account in reform and digitalisation projects of administration, and law drafting.
- We contribute to decision making in European collaboration.
- We promote the development of the EU's internal market within a shared legislative framework.

Vision

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

Our values

Community, creativity, fairness and impartiality

Data Protection Ombudsman Anu Talus:

Familiar themes in a changing environment

The themes of 2024 largely continued the trends of previous years, although with minor differences in emphasis. The new European Commission began its work and new digital regulation entered into effect. As usual, several Data Protection Ombudsman decisions, court rulings and European Data Protection Board (EDPB) guidelines and opinions were issued during the year. Unfortunately, the year was also marked by a number of data breaches.

The topic of AI has dominated both data protection seminars and public discourse. The AI Act was adopted in the EU in spring, entering into force in August 2024. Artificial intelligence models are often based on the processing of personal data, or an AI solution processes personal data. In such cases, a data protection authority is always entitled to supervise the processing of personal data. National work for enforcing the AI Act was also launched. In the preparation process, it is essential to ensure that, to the extent that the new regulation overlaps with the GDPR, supervisory responsibility remains with the Data Protection Ombudsman, with appropriate resources. For its part, the EDPB issued an opinion on AI in which it considered, among other things, that the use of personal data to train AI models may in certain situations be based on a legitimate interest. The opinion ensures that the GDPR is interpreted in the same way when assessing AI solutions.

New rules on the transparency and targeting of political advertising were adopted in 2024. As a result, new areas of oversight will also fall under the purview of the Data Protection Ombudsman. Many other legislative projects were also completed and new projects were launched. The approaching midway point of the government term was reflected in an increase in the number of requests for opinions. During the year, the Office of the Data Protection Ombudsman issued 55 opinions on legislative projects to ministries and 35 written expert opinions to parliamentary committees.

One of the issues that had a major impact on the field of data protection was the European elections and the resulting new Commission. The new Commission stated that it will reduce regulation, partly on the basis of recommendations made in the Draghi report. The report proposes a range of measures to improve Europe's competitiveness. The goal is to improve the position of small and medium-sized enterprises and create better conditions for innovation.

The EDPB continued its work in developing guidance and promoting the harmonised implementation of regulation. The guide published by the EDPB for small and medium-sized enterprises was translated into 18 different languages, including Finnish and Swedish. The EDPB also started making short, one-page visual summaries of its long guidelines. In addition, the EDPB highlighted another key aspect: the harmonisation of enforcement, as the proper functioning of the internal market requires a uniform application of regulation throughout the EU.

At the moment, the regulatory framework of data protection forms a complex entity, in which national authorities and European Union bodies have their own roles. These functions need to work together. Special attention has been given to this in national legislative projects.

In closing, let's take a brief look at the future. The Ministry of Justice has appointed a working group to work on the introduction of administrative penalties for the public sector in accordance with the Government Programme. This has been the objective of the Data Protection Ombudsman for several years. It is important to close the gap in the system of sanctions to ensure its consistency, effectiveness, fairness and deterrent capacity. Another project, which deals with a fundamental issue, concerns the use of dactyloscopic data from the passport register in criminal investigations.

"National work for enforcing the AI Act was also launched. In the preparation process, it is essential to ensure that, to the extent that the new regulation overlaps with the GDPR, supervisory responsibility remains with the Data Protection Ombudsman, with appropriate resources."

At the beginning of his term, the President of the United States has already repealed a number of regulations enacted during the previous administration. However, the data protection framework negotiated by the European Commission remains in place. It allows personal data to be transferred from EU countries to the United States. In the summer, the Commission published its first annual assessment of the functioning of the data protection framework and the EDPB published its own report in November.

It is also interesting to see where the deregulation projects launched by the Commission will ultimately lead. Are the so-called omnibus projects planned by the Commission, in which slight adjustments are being made to a few provisions of the GDPR, sufficient or is there a need for more extensive examination? Omnibus projects are extensive legislative packages that consolidate several different initiatives into a single legislative package. The GDPR may also be simplified as part of these.

One thing is certain – data protection will never get boring.

Anu Talus
Data Protection Ombudsman

Deputy Data Protection Ombudsman Heljä-Tuulia Pihamaa:

A varied year for data protection in the private sector

It was another busy and varied year for data protection in the private sector. Key decisions included the decision to prohibit the processing of personal data by a provider of loan comparison services and to issue three administrative fines. In particular, data breaches and contacts concerning data subjects' rights were a major concern for the private sector guidance and supervision unit.

The year also included guidance for controllers, an audit of the biobank in cooperation with Fimea and the first accreditation of a supervisory body for a code of conduct. From the Administrative Court, we obtained important decisions on issues such as the processing of health data by insurance companies and consent for cookies.

Although AI issues were discussed in the operating environment, the topic was not yet very visible in private sector supervision. We expect this to change at the latest when the phased application of the EU's AI Act, which entered into force in August 2024, starts in 2025. This will also bring new tasks for the Office of the Data Protection Ombudsman.

As in previous years, the financial sector was the largest group in the private sector. In the financial sector, where information relating to individuals' private lives is typically processed extensively, the obligation to handle personal data with care is heightened. In cybercrime, various vulnerabilities in information systems are constantly being identified and exploited, which is why regular assessment of the security and privacy of e-services is critical, especially in the financial sector.

As a cautionary example of inadequate security, a company providing loan comparison services was fined for breaching its obligation to protect personal data. In the same case, a hitherto rarely used power was used when the Deputy Data Protection Ombudsman prohibited the company from processing the data of loan applicants in the service after security flaws were discovered.

A major change in the financial sector took place with the introduction of the Positive credit register in spring 2024. This reform requires creditors to report information on all loans they grant to individuals to the Positive credit register, and to check the information stored in the register when assessing the creditworthiness of a consumer. The Data Protection Ombudsman has stressed the importance of data accuracy in the context of the preparation of legislation for the Positive credit register. These are important decisions that affect people's lives, so they must be based on correct and adequate information.

As data breach notifications are by far the largest group of issues for our office, we have wanted to pay special attention to the process of handling them. In order to speed up the processing of notifications and response to the ever-increasing number of them, we launched a development project focusing on data breaches. One of the key objectives is to explore how automation could be used in the processing of notifications. Work on this will continue intensively in 2025.

In the year under review, we took on new tasks when the EU Digital Services Act became fully applicable in February 2024. The Act imposes obligations on digital service providers to improve the transparency and security of services. The tasks of the Data Protection Ombudsman include monitoring the identifiability of non-profit and social advertising, the transparency of online advertising and recommender systems, and the protection of minors on online platforms. In Finland, enforcement of the Act is divided between the Finnish Transport and Communications Agency (Traficom), the Data Protection Ombudsman and the Consumer Ombudsman. This underlines the already smooth cooperation between the supervisory authorities, which I think has started very well.

The two-year EU-funded project *GDPR4CHLDRN – Ensuring data protection in hobbies*, a collaboration between the Office of the Data Protection Ombudsman and the TIEKE Finnish Information Society Development Centre, was completed at the end of the year. The outcome is the website tietosuojaharrastuksissa.fi, where associations involved in hobbies can find help on complying with data protection legislation in several languages. Although the materials focus specifically on hobbies, they are also useful for processing the personal data of children and young people in other situations.

The importance of Data Protection Officers and the adequacy of resources were also addressed when we supplemented the guidance on our website, based on the European Data Protection Board's report on the role of Data Protection Officers published in January 2024. We reminded organisations of the independence and resource requirements of Data Protection Officers, and that a Data Protection Officer should not be dismissed or penalised for performing his or her duties. A smart organisation understands that the Data Protection Officer or his or her team will always be involved as early as possible in any data protection issues.

Heljä-Tuulia Pihamaa
Deputy Data Protection Ombudsman

Deputy Data Protection Ombudsman Annina Hautala:

2024 – a year of major issues

What personal data is really necessary for different purposes? How to ensure that data moves securely and appropriately? How to reconcile data protection and privacy with other fundamental rights? These issues have been central to the guidance and supervision of public sector data protection in 2024 due to, among other things, a number of legislative projects affecting public administration.

The list of issues could be extended to include many others, such as how to ensure the security of the processing of personal data at all times. Unfortunately, there were also challenges on the public sector side during the year. A significant case was the data breach in the City of Helsinki in the spring. In a changed security and operational environment, it is even more important to recognise that personal data can be misused in ways that seriously compromise the security of individuals and society as a whole. It is also necessary to consider how to ensure that the information held by an organisation can actually be used. The value of information is reduced if it is not sufficiently structured, reliable or up to date.

As in previous years, in 2024 social welfare and health care constituted the largest sector in the Office of the Data Protection Ombudsman in terms of the number of new cases. In 2024, around one quarter of new cases concerned this sector. The lion's share of the cases involving public administration related to personal data breaches and the exercise of individuals' data protection rights, such as the access to, rectification or erasure of data. During the year, for example, a decision was adopted on the inclusion of personal data in text messages automatically sent to patients.

In addition to its supervisory and decision-making activities, the Office of the Data Protection Ombudsman supports both individuals and organisations by providing guidance through its website, in writing, by telephone and through participation in events and discussions. During 2024, around 2,300 guidance calls were answered, just over 1,200 written guidance responses were provided, and more than 180 speeches, media contacts and press releases were handled. As part of the guidance work, content targeted at the

healthcare sector was revamped on the website. The website now takes into account the revised Act on the Electronic Processing of Client Data in Healthcare and Social Welfare, the most recent decisions and case law.

In 2024, we also made use of audits targeted at organisations in our supervisory activities. These audits aim to identify areas for improvement before the risks to personal data have materialised. During the year, audit activity focused in particular on how organisations manage access rights and control the processing of personal data. During the year, the first joint inspection between the Office of the Data Protection Ombudsman and the Intelligence Ombudsman was carried out, and inspection activities were extended to the healthcare sector. Based on the audit findings, guidance and recommendations were given to the organisations.

A noteworthy feature of the year is the significant increase in the number of statements issued to prosecutors or pre-trial investigation authorities, from 54 in the previous year to 111 in 2024. Most of the statements concerned data protection offences, data breaches and violations of the confidentiality of communications. The overall picture of the so-called criminal case statements and security breach notifications is worrying in terms of the number of hacking cases, bearing in mind that many such cases remain hidden.

The use of artificial intelligence and digital tools was a key theme during the year, including in the public sector. In the early childhood education and education sector, for example, this was reflected in the number of statements requested. For example, the Office of the Data Protection Ombudsman issued a statement on a draft guide on the use of AI applications in the processing of learners' personal data. The above-mentioned statement also highlighted the importance of teaching learners, as a civic duty, to understand how their personal data is typically processed in web-based AI services and what their rights are.

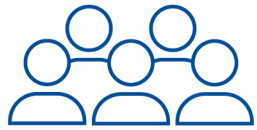
I began my text with the big issues that were considered in 2024. One key pair of issues not mentioned at the beginning is how AI will affect the future and how data protection can be ensured when using it. This pair of issues was already raised in 2024, but both this and the issues stated at the beginning will remain relevant in the years to come.

Annina Hautala
Deputy Data Protection Ombudsman

Office of the Data Protection Ombudsman's year 2024 in figures

13,284
Cases instituted

13,291
Cases processed



60
Number of personnel at end of year

In 2024, the Office of the Data Protection Ombudsman issued

- **3** decisions imposing administrative fines for data protection violations
- **18** reprimands for processing measures that violated data protection legislation
- **9** orders to bring personal data processing measures into compliance with the GDPR
- **5** orders to fulfill the rights of the data subject
- **42** orders to notify data subjects about a personal data breach
- **2** warnings concerning planned processing activities that would probably violate the GDPR

7,152

Personal data breach notifications

9

Audits initiated or carried out

2,289

Calls answered by the telephone service

55

Statements on legislative projects

110

Statements to prosecutors and pre-trial investigation authorities

7

Lead supervisory authority in cross-border cases

252

Supervisory authority concerned in cross-border cases

Events in 2024

JANUARY

- The European Data Protection Board (EDPB) published a report on a coordinated investigation related to data protection officers
- The Data Protection Day event was held in Helsinki
- The Administrative Court upheld the Data Protection Ombudsman's decisions on the health data processing of insurance companies

FEBRUARY

- The EU's Digital Services Act (DSA) entered into force
- The coordinated initiative of the European data protection authorities on investigating the implementation of the right of access was started
- The EDPB issued a statement on the draft CSAM Regulation

MARCH

- An administrative fine was imposed on Verkkokauppa.com for not defining a storage period for customer data
- The Deputy Data Protection Ombudsman issued a decision on including personal identity codes in text messages sent to patients automatically
- A temporary personal data processing ban was imposed on Sambla Group
- The Supreme Administrative Court confirmed a decision ordering Google to remove links from search results

APRIL

- The Positive credit register was launched
- The EDPB issued a statement on the 'consent or pay' models used by social media platforms
- The Expert Board of the Office of the Data Protection Ombudsman was appointed for the next three-year term

MAY

- Investigation of the City of Helsinki personal data breach was started
- The data protection authorities of the Nordics met in Norway
- The Deputy Data Protection Ombudsman issued a decision on the storage periods of telecommunications companies' customer data

JUNE

- Guidance for organisations that appoint a data protection officer was updated
- The *Data protection in hobbies* website was launched under the GDPR4CHLDRN project
- The EDPB issued a statement on facial recognition at airports
- The Supreme Administrative Court confirmed a decision according to which a link did not need to be removed from Google search results

JULY

- The European Commission published its four-year report on the application of the GDPR
- The EDPB issued a statement on the role of data protection authorities in the AI Act framework
- The Deputy Data Protection Ombudsman concluded that publishing personal phone numbers on a company's intranet was illegal

AUGUST

- The EU's AI Act entered into force

SEPTEMBER

- The EDPB's Data Protection Guide for Small Companies was published in Finnish and Swedish
- A decision related to the Legal Register Centre's disclosure of incorrect payment default data was upheld
- The Finnish Tax Administration was ordered to remedy its deficient procedure in the implementation of the right of access

OCTOBER

- The data protection authorities of G7 countries highlighted the role of data protection supervisory authorities in AI supervision
- The Supreme Administrative Court partly upheld a decision of the Deputy Data Protection Ombudsman related to the Ministry of Foreign Affair's reporting obligation
- The Deputy Data Protection Ombudsman issued a decision on the application of the GDPR on the traffic data of mobile plans
- The EDPB published a draft guideline on legitimate interest
- The EDPB issued a statement on personal data processors

NOVEMBER

- An administrative fine was imposed on Posti for data protection deficiencies found in the OmaPosti service
- The EDPB published its first report on the EU-US Data Privacy Framework

DECEMBER

- An administrative fine was imposed on Sambla Group and the company was ordered to notify its customers of the data protection breach
- The EDPB issued a statement on considering data protection in the context of AI models
- The EDPB published a draft guideline on the disclosure of data to authorities of non-EU countries

Focus areas of data protection work

Case volumes, development measures and new tasks

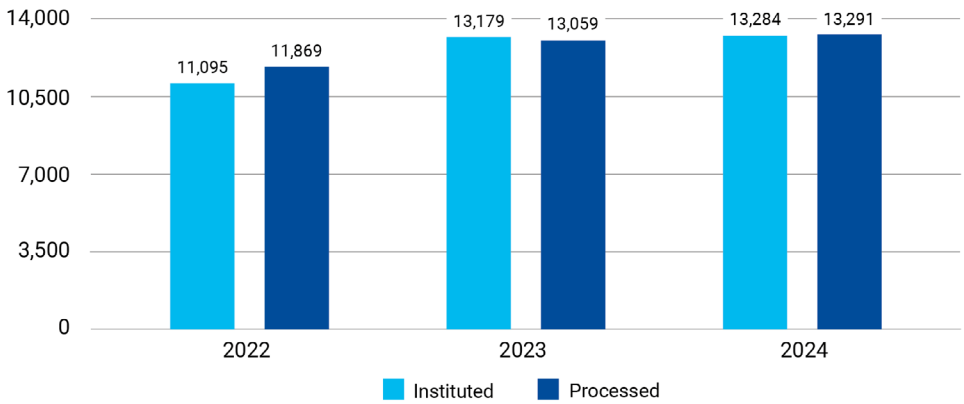
The number of pending cases continues to rise

The number of cases pending at the Office of the Data Protection Ombudsman remained at the high level of the previous year and continued to increase. In 2024, a total of 13,284 new cases were instituted. A total of 13,291 cases were closed, which is some 200 cases more than in the previous year.

Reports of personal data breaches have been the largest category of cases for several years now. A total of 7,152 personal data breaches were reported to the Office in 2024.

The Office has worked to reduce the number of pending cases since 2020. At the end of 2024, there were around 1,200 pending cases that were instituted more than two years ago, between 2018 and 2022. Most of these are related to issues that must be processed in cross-border cooperation and where the process is headed by a data protection authority of another EEA country. Despite the increase in the number of cases, the work to reduce the number of pending cases has produced results.

Matters instituted and processed from 2022 to 2024



Case processing improved with development measures

The key development targets of the Office include making the preparatory work of case resolution and matters brought to the Sanctions Board more effective. The amendments to the Data Protection Act that entered into force at the start of 2024 enable the Data Protection Ombudsman to delegate decision-making power in certain strictly defined cases as laid down in the Office's rules of procedure. Two presenting officers that may decide cases were appointed in autumn 2024. During the year, development of the activities of the Sanctions Board was started and a position for a senior officer specialising in preparing cases for the Sanctions Board was created. The Sanctions Board is responsible for processing cases that may require imposing an administrative fine or a ban on processing personal data.

In 2024, the Office started a development project for the purpose of developing the case flow management of personal data breach notifications. Since the application of the GDPR started, more than 30,000 personal data breaches have been reported to the Office of the Data Protection Ombudsman. The development project involves investigating the use of automation in the processing of personal data breach notifications, among other matters.

The personal data breach notification screening procedure introduced in 2022 has been found to have made the processing of the notifications significantly more efficient. Among other tasks, the screening involves assessing whether a case requires more detailed investigation with the controller and whether a case requires action from authorities. The process was further improved in 2024.

The screening of cases pertaining to data subject's rights was also continued. The procedure has been applied to cases related to social welfare and healthcare services since 2022, and the practices were updated with changes that support the case flow management for this sector. In September 2024, the screening procedure was extended to cover cases related to the financial sector. The procedure allows investigating matters related to the rights of data subjects' soon after they are instituted, for example. The aim is to extend the screening to cover all other sectors as well.

Improving information management has been set as a key objective for the near future. The joint case management system for agencies in the judicial administration introduced in 2023 has made case and information management at the Office of the Data Protection Ombudsman more effective. The system has better reporting and monitoring functions and provides better statistical information than the previous system. The information can be made use of in resource planning and other operational management.

Legislative amendments introduce new tasks

Several new tasks have been introduced for the Office of the Data Protection Ombudsman in the recent past because of legislative amendments, and the number of tasks is expected to increase.

The amendments to the Data Protection Act (1050/2018) and the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018) entered into force at the start of 2024. The amendments require the Office to resolve all complaints or give the complainant an estimate of when a decision will be issued within three months of the case being instituted. Data subjects can lodge a complaint with the Administrative Court if the Data Protection Ombudsman does not issue a decision or give an estimate of the processing time within this deadline. The amendments apply to cases that are instituted after the start of 2024 and it does not apply retroactively. In 2024, around 3,130 cases were instituted at the Office to which the provisions on appeals against inactivity are applied. The cases are mainly notifications, complaints, requests for advice and matters related to data subjects' rights. Most of the cases were resolved before the three-month deadline was passed.

After the Finnish whistleblower act (*1171/2022*) entered into force at the start of 2023, the Office of the Data Protection Ombudsman became the competent supervisory authority in terms of privacy and personal data protection and notifications related to the security of information systems. Competent authorities must annually report to the Office of the Chancellor of Justice on notifications made under the Finnish whistleblower act. During the year, the Data Protection Ombudsman received six notifications falling under the Ombudsman's authority. Six notifications were also investigated and resolved. One of the resolved notifications was made in 2023. The notifications were deemed to not give cause to take measures.

The EU's renewed digital and data regulations introduce new tasks for the Office of the Data Protection Ombudsman.

The EU's renewed digital and data regulations also introduce new tasks for the Office of the Data Protection Ombudsman. The digital and data regulations include the AI Act (AIA), the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Act (DA) and the Data Governance Act (DGA).

The DSA became fully applicable on 17 February 2024. It lays down responsibilities for providers of digital services such as online platforms on improving the transparency and security of services. In Finland, supervision under the DSA is divided between the Finnish Transport and Communications Agency Traficom, the Office of the Data Protection Ombudsman and the Consumer Ombudsman. Traficom has the primary responsibility. The Data Protection Ombudsman supervises the identifiability of non-commercial and societal advertising, the transparency of online advertising and recommender systems, and the protection of minors on online platforms. The DSA forbids targeting advertising on online platforms based on special categories of personal data, such as political opinion, religion or ethnic origin, and targeting advertising to minors based on personal data. Finnish authorities received 78 complaints under the DSA in 2024. Three of them were lodged with the Data Protection Ombudsman.

Matters related to AI were strongly present in the operational environment. The EU AI Act entered into force in August 2024 and its application will be started in stages. EU countries must designate the national authorities responsible for the supervision under the AI Act by 2 August 2025. During the year, the European Data Protection Board issued statements on the development of AI models and the role of data protection authorities in the supervision of high-risk AI systems. In October, the data protection authorities of the G7 countries issued a statement in their meeting in which they highlighted the vital role of data protection authorities in the supervision of AI.

Number of notifications on data breaches is still high

Notifications related to personal data breaches are the largest individual category of cases that are instituted at the Office of the Data Protection Ombudsman. In 2024, 7,152 notifications of personal data breaches were submitted, which is some 250 more than in the previous year. Personal data breaches must be notified to the Office of the Data Protection Ombudsman if the breach can cause a risk to the individuals affected. The notification must be submitted without delay and at the latest within 72 hours of the time the breach is discovered.

The number of personal data breaches has increased in the recent years and in 2024, 54% of all new cases were personal data breaches. The number is similar to the numbers of Finland's peer EU countries. The increase is partly caused by the increasing digitalisation and advancements in information technology. General awareness of the duty to notify personal data breaches has also increased. Most notifications are submitted by operators in regulated sectors, such as social welfare and healthcare services and the financial sector.

One of the most serious personal data breaches was the City of Helsinki breach that was discovered in April 2024. The City of Helsinki notified the Office of the Data Protection Ombudsman on 30 April of a personal data breach, which affected learners, their guardians and the City's employees. The Data Protection Ombudsman is investigating the personal data breach from the perspective of compliance with data protection legislation. The Police of Finland is investigating the case.

The number of personal data breaches has increased in the recent years and in 2024, 54% of all new cases were personal data breaches.

Several cyberattacks targeted the hospitality and tourism sector during the year, and some of these led to the perpetrators gaining the admin credentials of booking systems. Personal data of customers was stolen from the booking systems and the data was used in phishing scams. Special to these attacks was that in addition to phishing emails, the perpetrators also phished for the admin credentials by creating fraudulent booking system admin portals, which they managed to include in Google search results.

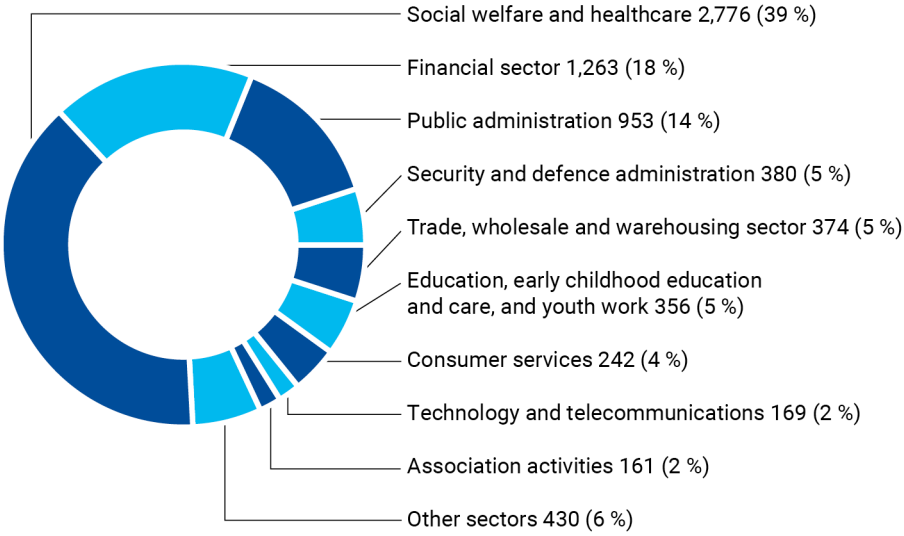
Often, personal data breaches could be prevented with appropriate technical measures, appropriate organisational practices and by ensuring a sufficient level of data protection competence. Old and out of date devices and systems and, in particular, deficiencies in information security cause a risk of a personal data breach. In addition, a trend has been found that vulnerabilities of

systems are taken advantage of faster than before. Often such breaches also affect personal data stored in the system. Telecommunications devices such as VPN devices and firewalls that serve as a connection between the internet and a company's internal network are particularly vulnerable to attacks.

Criminals use stolen user credentials in many ways. They can be used to log in to a service or make purchases in the victim's name, for example. Usually, attacks using user credentials involve making numerous login attempts with different combinations of usernames and passwords. As a security measure, users should always use different passwords in different services. In addition, organisations should limit the number of consecutive failed login attempts allowed.

Methods used to phish for user credentials and passwords are increasingly sophisticated as well. Using the Adversary-in-the-Middle (AiTM) technique has become more common, for example. AiTM allows the attacker to bypass multi-factor authentication, which makes protection more difficult. Information can also be sold and used for new crimes. For example, criminals can use user credentials stolen in a past attack and send phishing messages from familiar email addresses, making them seem genuine.

Personal data breach notifications instituted by sector, 2024



Cross-border cases and European cooperation

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.

The data protection authorities of the European Economic Area monitor the processing of personal data in cooperation.

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 (EDPB) has a register of joint decisions taken by data protection authorities on its website.

In 2024, the Office of the Data Protection Ombudsman was the lead supervisory authority in seven cases and a supervisory authority concerned in 252 cases. As a concerned supervisory authority, the Office also contributed to cases involving mediation, of which there were 100 during the year. The Office forwarded 39 cases to the joint procedure of authorities.

The Office of the Data Protection Ombudsman submitted one objection to a draft decision made by a lead supervisory authority. The case in question pertained to the implementation of a data subject's rights after a complaint had been lodged with the Office and the case was forwarded to another EU country for processing. In addition, the Office contributed to the content of the draft decision in several cases.

The Office of the Data Protection Ombudsman is active in the European Data Protection Board and its subgroups. The EDPB comprises the EU's national data protection authorities and representatives of the European Data Protection Supervisor. Finland's Data Protection Ombudsman Anu Talus is the chair of the Board from 2023 to 2028. As a member of the Board, the Office of the Data Protection Ombudsman contributes to the creation of guidelines and policies in collaboration with the supervisory authorities of other EU countries. The Board published several significant opinions and guidelines in 2024 that clarify and harmonise the application of the data protection legislation in current matters.

The opinions issued by the European Data Protection Board, which are binding on data protection authorities, pertained to AI models, the 'consent or pay' practices of large online platforms, determining the location of the main establishment of a controller, the use of processors and sub-processors, and facial recognition at airports. In the opinion issued on sub-processors in October, the Board clarified how certain duties of controllers laid down in the GDPR and the wording of controller-processor contracts should be interpreted. The Board concluded that the initial processor must ensure that its sub-processor meets the requirements for processing personal data. However, the controller ultimately makes the decision and bears the responsibility over using a specific sub-processor.

In its opinion on AI models, the Board discussed the use of personal data in the development and use of AI models. The opinion pertained to when an AI model could be considered anonymous, among other matters. For a model to be considered anonymous, it must not be possible to identify the individuals whose data was used to create the model and it must be impossible to extract personal data from the AI tool with queries. In addition, the Board assessed legal bases on which personal data can be processed and what should happen if an AI model is developed with unlawfully processed personal data. The Board also provided different methods and tools to support making assessments. Questions related to AI were also discussed in July, when the Board highlighted in its statement the vital role of data protection authorities in the supervision under the AI Act.

In June, the final version was adopted of the guidelines that provide guidance to the law enforcement authorities of EU countries in cases where they transfer data to the authorities of non-EU countries or international organisations.

The EDPB published several significant opinions and guidelines in 2024 that clarify and harmonise the application of the data protection legislation in current matters.

In October, guidelines were published that clarify which tracking technologies are included in the scope of the ePrivacy Directive. In December, draft guidelines were published that clarify the rules for data sharing with the authorities of non-EU countries. In the autumn, important draft guidelines were published on personal data processing based on legitimate interest. The guidelines define criteria that must be met if an organisation plans to process personal data based on its legitimate interest. In addition, the guidelines explain how the use of legitimate interest at a basis should be assessed in different situations.

The European Data Protection Board issued a statement on its opinion of the legislative amendments that the European Parliament and Council made to the draft Regulation of the European Commission that would lay down additional rules for the cooperation between authorities. The aim of the new Regulation is to streamline cooperation between European data protection authorities in processing cross-border cases. The Commission submitted the proposal for the Regulation in July 2023 after an initiative from the Board. The trialogue on the proposal was started 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 transferring personal data, the controller or the processor must ensure on a case-by-case basis whether a sufficient level of protection can be guaranteed for the personal data to be transferred.

In January, the European Commission published its first periodic review of 11 existing adequacy decisions that were adopted under the legislation preceding the GDPR. According to the Commission's assessment, all 11 countries and territories still provide a sufficient level of protection for personal data transferred from the EU. In addition, the Commission deemed that the data protection frameworks of these countries and territories have further converged with the EU's framework.

In March, the European Data Protection Board published its report on the functioning of the EU-US Data Privacy Framework. The report pertained to the European Commission's first periodic review of the adequacy decision in place for the United States. The Board concluded that the decision that has been applied since the summer of 2023 is functional and especially highlighted the significance of the redress mechanism contained in the decision. The Board also brought up some targets for development and called for monitoring the practical functioning of safeguards and matters related to the US's intelligence activities. The Data Privacy Framework allows transferring personal data between EU countries and US companies that have certified themselves under the framework.

During the year, the European Data Protection Board clarified the rules for data sharing with the authorities of non-EU countries or third countries. Third-country authorities can request data from organisations operating in the EU for the purpose of apprehending criminals, preventing attacks or monitoring financial transactions. The draft guideline published by the Board in December clarifies under which conditions it is lawful for organisations to respond to such requests and how personal data can be securely transferred.

The supervisory authorities of EU countries issued a decision after a cooperation procedure on the ride service Uber that clarified certain questions relating to data transfers. The Dutch data protection authority led the investigation and issued the decision, because Uber's European main office is in the Netherlands. The Office of the Data Protection Ombudsman also contributed to the decision making. A fine of EUR 290 million was imposed on the company because it was deemed to have transferred the personal data of European Uber drivers to the United States without ensuring a sufficient level of protection for a period of two years. Uber has appealed the decision.

Support to controllers and data protection officers

Report on the implementation of the right of access

The Office of the Data Protection Ombudsman collaborated with 30 European data protection authorities in a series of actions coordinated by the European Data Protection Board that focused on investigating how data subjects' right to access personal data collected on them is implemented by different organisations. The investigation was started with a survey that the Office sent to 15 organisations in Finland in March 2024. The investigation targeted cities and wellbeing services counties as well as companies from several industries, among others. In total, responses were received from 1,185 organisations of different sizes from around Europe.

The European Data Protection Board published a report on the investigation in January 2025. The report describes the identified challenges and provides recommendations on what organisations should consider when implementing the right of access. The report discusses seven of the identified challenges in more detail. These include deficiencies in the organisation's internal documentation, restricting the right of access with incorrect grounds, and barriers that a data subject may face when attempting exercise their right of access. The Board provides recommendations for overcoming each challenge.

Based on the results, two in three data protection authorities assessed the level of organisations' compliance with the right of access as 'average' or 'high'. For example, many organisations have introduced online services that individuals can use to submit a request easily or download their data. The results show that larger organisations are better equipped to fulfil access requests than smaller organisations. The national results of the survey are included as an appendix to the report.

Supervisory authorities decide the further measures required nationally based on the findings. Instructions for organisations based on the findings for Finland were added to the website of the Office of the Data Protection Ombudsman. The added instructions included information on the format the data must be provided in, how long the requests must be retained, and what must be considered when the identity of the individual making the request is verified. The website also clarifies what should be done when the data to be provided also includes personal data belonging to another data subject or if an individual requests access on behalf of another individual.

Instructions for organisations that have designated a data protection officer were updated

The Office of the Data Protection Ombudsman updated the instructions on its website aimed at organisations and managers that have appointed a data protection officer. The updated instructions remind organisations that a data protection officer's role must be independent and they must be provided with the appropriate resources.

The instructions were updated based on the report published by the European Data Protection Board in January 2024 on the investigation of the role of data protection officers. According to the report, many data protection officers still face challenges in their duties. The updates the Office made to the instructions on its website were part of the national measures implemented because of the report. Tailored instructions were also provided to six controllers that responded to the survey.

Instructions on data protection in the hobbies of children and young people were drawn up in the GDPR4CHLDRN project

The two-year, EU-funded *GDPR4CHLDRN – Ensuring data protection in hobbies* project of the Office of the Data Protection Ombudsman and the TIEKE Finnish Information Society Development Centre ended in the autumn of 2024. The aim of the project was to improve the data protection skills of children between 13–17, their parents and organisations organising hobby activities.

The website Data protection in hobbies (tietosuojaharrastuksissa.fi) was launched in June as a home for the material created in the project. The most extensive part of the material is the practical guide aimed at the boards of associations organising hobby activities. The materials support the associations in their application of and compliance with data protection legislation and include many examples inspired by everyday occurrences in hobbies. Dedicated instructions were also created for coaches and instructors, children and young people, and parents. The website also has tests for assessing one's skill level.

The website is in Finnish, English and Swedish. To ensure that the instructions are accessible to as large an audience as possible, the key materials were also published in Arabic, Estonian, Northern Sami, Russian and Somalian.

The materials were created in collaboration with different target groups. During the year, data protection training and webinars were held for people involved with hobby activities. In addition, a final survey was used to assess the general skill level in data protection and attitudes towards it. A total of six newsletters were sent under the project during the year, which reached more than 300 interested parties at their highest. In addition, the project took part in the Media Literacy Week and the ITK Conference focusing on digital education and learning. A total of 12 articles and blog posts were published during the year.

The EU Citizens, Equality, Rights and Values Programme (CERV) funded the project. Stakeholders of the project included the Guides and Scouts of Finland, the Football Association of Finland, and the Finnish Olympic Committee.

Supervision and collaboration

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 2020–2024, the Sanctions Board has imposed a total of 23 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.

The Ministry of Justice's ongoing legislative drafting project assesses the penalty system applied to violations of data protection legislation. The current Government Programme includes an entry on extending the current system of administrative fines to the public sector as well. The consultation round on the assessment memorandum was started in March 2024. In the statement the Office of the Data Protection Ombudsman issued on the assessment memorandum, the Office repeated its view that the change is necessary to ensure the consistency, effectiveness, fairness and dissuasiveness of the penalty system. In the Office's view, the legal liability of public officials and criminal sanctions alone are not sufficient to ensure that public administration appropriately complies with the responsibilities arising from data protection legislation. Currently, public sector operators can be fined in all other Nordic countries.

An administrative fine was imposed on three organisations in 2024. The fines were issued for not defining a storage period for customer data and unlawfully requiring registration, the data protection deficiencies in the OmaPosti service, and the neglect of data security by loan comparison services. The amounts of the fines were between EUR 856,000 and 2.4 million.

In 2024, the Sanctions Board imposed an administrative fine to three organisations for violations of data protection legislation.

- An administrative fine of EUR 856,000 was imposed on Verkkokauppa.com because the company had not defined how long the user account data of online customers will be stored. In addition, the company's practice of requiring the creation of a user account in order to place an order online was contrary to data protection legislation. The Data Protection Ombudsman ordered Verkkokauppa.com to define a storage period for user account data and to remedy its practice of mandatory registration. In a decision issued in February 2025, the Helsinki Administrative Court lowered the amount of the fine to slightly above EUR 792,000 on the grounds that it should have been based on the company's 2023 turnover instead of its 2022 turnover. The Administrative Court's decision is not final.

- Posti was imposed an administrative fine EUR 2.4 million for the data security deficiencies of the OmaPosti service. Posti had automatically created an electronic OmaPosti mailbox for its customers without separate request. The electronic mailbox could not be closed without losing access to all other functions of the service, such as redirecting post to another address and the My Pickup Point function. The OmaPosti service also had technical settings that did not meet data protection requirements, such as an automatically enabled switch and a box that was ticked by default. Posti was ordered to remedy its practices. The decision is not final.

- Sambla Group, which provides loan comparison services, was imposed an administrative fine of EUR 950,000 because the contents of its customers' loan applications were accessible to third parties through the personal links intended for the customers because of the company's weak information security. The Deputy Data Protection Ombudsman also ordered Sambla Group to notify its customers of the incident whose data third parties may have been able to access. The decision is final.

Auditing activities

Audits are one of the measures available for the Office of the Data Protection Ombudsman to detect deficiencies in data protection and to guide organisations to comply with data protection legislation. They are also an effective method for supervising compliance with the orders of the Data Protection Ombudsman. Audits are carried out both according to the annual plan and when necessary. The Data Protection Ombudsman's auditing activities are steered by the risks related to personal data processing, an identified need to monitor a certain controller or sector, and inspection obligations arising from legislation. The auditing activities of 2024 focused on the supervision of personal data processing in organisations and user right management.

Five audits were carried out in 2024. In addition, four unfinished audits or inspections planned for 2024 were postponed to 2025. 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 audits.

As usual, the 2024 audits targeted security authorities, because data subjects only have a limited capability to monitor the data processing carried out by them. For example, the Office of the Data Protection Ombudsman and the Intelligence Ombudsman carried out their first audit together that targeted the Finnish Security and Intelligence Service. The audit targeted the personal data processing related to intelligence activities insofar as data is saved in the Finnish Security and Intelligence Service's information systems or other storage platforms.

The Data Protection Ombudsman examined the implementation of data protection in the security sector, health care and biobanking in 2024.

During the year, the Office extended its auditing activities to cover healthcare services as well. The audit of HUS involved assessing the supervision of patient data processing and, in particular, the controller's measures to detect any patient data processing that violates the GDPR. The audit targeted the supervision of patient data use log information in 2023 and 2024.

In autumn, the Office of the Data Protection Ombudsman and the Finnish Medicines Agency Fimea collaborated to inspect the Helsinki Biobank. Based on the findings, the Biobank was instructed to read the instructions on personal data breaches and to provide the bases of personal data processing as clearly as possible in the information provided to individuals. In addition, the Biobank was instructed to assess the risks associated with technical method development for individuals and to ensure that the roles and responsibilities in its personal data processing are clear when the personal data collected for the biobank activities is processed in HUS's data pool.

Private sector

In decisions pertaining to private sector operators, questions related to data subjects' rights, data storage periods and publishing data were the most common. More information on the three decisions that the Office of the Data Protection Ombudsman's Sanctions Board issued to companies is in the section titled 'Sanctions Board'.

The Deputy Data Protection Ombudsman deemed in May that a telecommunications company had the right to store the data of their mobile plan customers for three years after the customer relationship ends. The length of the period is related to debts becoming time-barred in three years in Finland. If the data was erased earlier, the company could be placed in a situation where it is not able to defend itself if a customer or other creditor makes a claim based on an error. However, the Deputy Data Protection Ombudsman reprimanded the telecommunications company because it had not erased personal data of a customer whose customer relationship had ended more than ten years ago despite the customer's request. The decision is final.

In September, the Deputy Data Protection Ombudsman reprimanded another telecommunications operator because the company had delivered only some of the information requested by the data subject and mostly on paper via post, even though the data subject requested to receive the information in an electronic format. In the decision, the Deputy Data Protection Ombudsman also deemed that the traffic data of a mobile plan can also be considered personal data. The decision is final.

In June, the Deputy Data Protection Ombudsman outlined that a company did not have the right to publish its employees' personal phone numbers on its intranet. There was no legal basis for disclosing the personal data to third parties and contact between the employees could have been enabled by using work phones, for example. The company was reprimanded. The decision is final.

During the year, administrative courts confirmed several decisions issued by the Office of the Data Protection Ombudsman. The decision of the Administrative Court on the administrative fine imposed on Taksi Helsinki became final in May after the Supreme Administrative Court did not grant leave to appeal. The Office of the Data Protection Ombudsman's Sanctions Board had deemed in 2020 that the company had not assessed the risks associated with its personal data processing before it introduced a surveillance camera system to its taxis that recorded sound and video. The Administrative Court lowered the amount of the administrative fine and repealed one of the orders of the Deputy Data Protection Ombudsman. For all other parts, the Deputy Data Protection Ombudsman's decision remained effective.

The Supreme Administrative Court upheld two decisions of the Office of the Data Protection Ombudsman related to the removal of Google search result links. In March, the Supreme Administrative Court ordered Google to remove links to articles from news media from its search results. The Deputy Data Protection Ombudsman had deemed in June 2020 that including the links in the search results was no longer justified. In May, a decision issued by the Data Protection

Ombudsman in April 2022 was confirmed. The decision stated that Google did not need to remove a link to an opinion piece from its search results. The information in the opinion piece was information that the person had made public independently by taking part in public debate. The search result did not portray the person in any materially incorrect, deficient or misleading way. The Administrative Court did not amend the Data Protection Ombudsman's decision and the Supreme Administrative Court did not grant leave to appeal.

The decisions of the Administrative Court also provided the Court's view on questions related to requesting consent for cookies. The Office of the Data Protection Ombudsman submitted statements in two cases pertaining to cookies to the Finnish Transport and Communications Agency Traficom and the Helsinki Administrative Court. The Administrative Court rejected the appeals that Telia and Sanoma Media Finland had lodged on two Traficom decisions that related to requesting consent for cookies and assessing the necessity of cookies. The Administrative Court adopted the same view as the Data Protection Ombudsman and Traficom and deemed that banners used to request consent for using cookies must also have an equally visible option for refusing cookies. In addition, the Court deemed that users' consent must also be requested in Sanoma's news application for cookies related to providing personalised content and the cookies enabling Telia's chat function because these were not considered necessary cookies. The Administrative Court's decisions are not final.

The Deputy Data Protection Ombudsman accredited the first codes of conduct monitoring body in May. Codes of conduct are sector-specific practical guidelines for the application of data protection legislation that each sector creates for itself. In the private sector, compliance with codes of conduct is supervised by a monitoring body accredited by the Office of the Data Protection Ombudsman. The Finnish Bar Association and the monitoring board operating under it were accredited, or approved, as a monitoring body with certain conditions. The accreditation enters into force when the Finnish Bar Association submits its new code of conduct for the commissions of attorneys-at-law and the Office of the Data Protection Ombudsman approves it.

The European Data Protection Board provided its view on requesting consent for targeted advertising in social media. The Board issued a statement binding on supervisory authorities on the 'consent or pay' model used by large online platforms in which the Board stressed that users must be able to genuinely choose whether their personal data is used for targeted advertising. The Board welcomed the November announcement of a large online platform that it will change its model.

Financial sector

During the year, a current issue in the financial sector was the realisation of data subject's rights in the Positive credit register. The Positive credit register was launched in April 2024. The register comprises information on the credits and income of private individuals. The Office of the Data Protection Ombudsman supervises the personal data processing in the Positive credit register.

The Data Protection Ombudsman submitted a statement in June on the amendment of the act on an income information system (*Laki tulotietojärjestelmästä 53/2018*) and the Act on the Positive Credit Register (739/2022). Currently, personal data can be disclosed from the Incomes Register and the Positive credit register even if a data subject has requested that the disclosure of their incorrect data is temporarily prevented. The Data Protection Ombudsman stressed that there can be no compromise on the accuracy of data when decisions that have a significant impact on a data subject are made. The Data Protection Ombudsman had highlighted this issue already previously, when the Act on the Positive Credit Register was being drafted.

The two acts are being reviewed because of the Data Protection Ombudsman's observations and the views presented by the Chancellor of Justice in their pre-review. According to the current version of amendments, users of the Incomes Register and the Positive credit register would be informed that the data subject has requested that some of their personal data is not disclosed. However, according to the proposed amendments, such data would still be disclosed from both registers regardless of the data subject's request.

The Data Protection Ombudsman also issued a statement on the amendments proposed to the Act on the Positive Credit Register in December. The amendments would add information on the shareholder-specific loan shares of housing company loans to the Positive credit register. The Data Protection Ombudsman endorsed the proposal to leave out the name and Business ID of the housing company from credit reports. In the same context, the Data Protection Ombudsman also noted that all creditors are provided with the same data from the register and that the draft amendment act does not include provisions on restricting data content based on the creditor. This means that banks and companies providing short-term loans receive the same information. The Data Protection Ombudsman proposed that the amendment act be reviewed again to find a solution where creditors would only receive the data that is necessary for their operations.

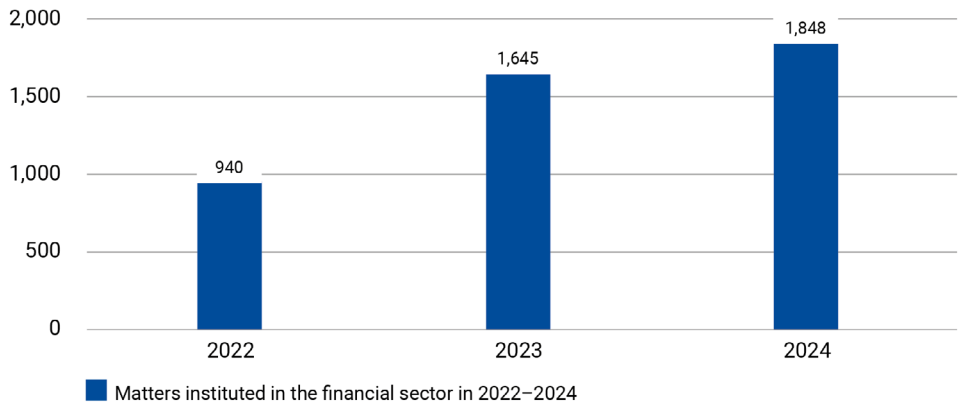
The requirement for due diligence in personal data processing is particularly important in the financial sector because the operators in the sector often extensively process information pertaining to individuals' private lives. This is why assessment of information security and data protection is important in electronic services. The Deputy Data Protection Ombudsman brought this up in the decision issued in December on Sambla Group. The deficiencies in the company's information security were found in the company's lainaparkki.fi and rahoitu.fi services. The customers of these services were sent links through which third parties could access the loan applicant's contact details and details about their income, housing expenses, marital status and possible children, for example. In March 2024, as

soon as the severity of the information security deficiencies became apparent, the company was ordered to stop processing loan applicants' personal data in its electronic services. In December, an administrative fine was imposed on the company and it was ordered to improve its information security.

A decision of the Deputy Data Protection Ombudsman in a case pertaining to disclosing incorrect payment default data was confirmed by a court in August. In November 2021, the Deputy Data Protection Ombudsman had ordered the Legal Register Centre to remedy its procedure for monitoring the correctness of the payment default data it disclosed to credit information companies. Information based on judgements issued in civil cases should not have been entered as payment default entries in the Positive credit register in cases where the payment obligation was justifiably disputed. The Administrative Court upheld the Deputy Data Protection Ombudsman's decision as it was, and the Supreme Administrative Court did not grant leave to appeal.

In January, the Administrative Court upheld the Data Protection Ombudsman's decisions pertaining to the processing of health data by two insurance companies. The decisions were related to requesting data from healthcare services and processing health data of insurance policy applicants. The Data Protection Ombudsman had observed in 2022 that insurance companies had requested unnecessarily extensive amounts of health data from healthcare services and the insurance companies did not have any bases for processing the health data of the insurance policy applicants before signing an insurance agreement. The decisions of the Administrative Court have been appealed against to the Supreme Administrative Court.

Matters instituted: Financial sector



Public sector

The largest share of public sector cases was related to personal data breaches and the use of the legal remedies available to data subjects, such as the right of access or the right to erasure. In the public sector, the steering and monitoring activities are targeted at several subsectors and in addition to the GDPR and the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security, the legislation supplementing and specifying these must be applied.

Social welfare and healthcare

Social welfare and healthcare is the largest sector measured in the number of cases initiated at the Office of the Data Protection Ombudsman. In 2024, around 25% of all cases initiated were related to this sector. The social welfare and healthcare sector comprises both private and public operators, and the sector's cases are processed at the Office in the guidance and supervision units for both the public and private sectors.

Social welfare and healthcare is the largest sector measured in the number of cases initiated at the Office of the Data Protection Ombudsman.

Most of the cases were notifications of personal data breaches. The processing of these notifications was made more effective during the year. In addition, cases related to accessing, correcting and erasing client or patient data were a significant group, and the processing of these was made more effective with a screening procedure. The Office also receives many inquiries related to the personal data processing in the sector from both organisations and individuals.

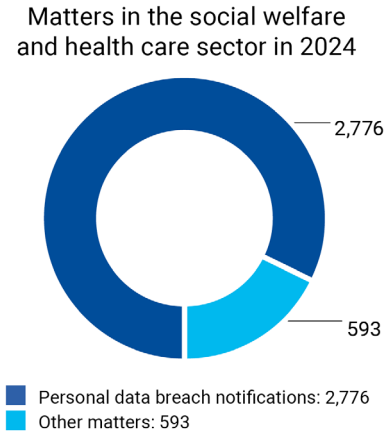
Because large quantities of sensitive data are processed in the sector, in addition to its supervision and decision-making activities, the Office supports social welfare and healthcare operators by providing general guidance on its website, for example. To this effect, the website content for the sector was updated during the year. In addition, the Office contributes to the organisation of the annual SohviTellu data protection seminar aimed at data protection professionals working in social welfare or healthcare.

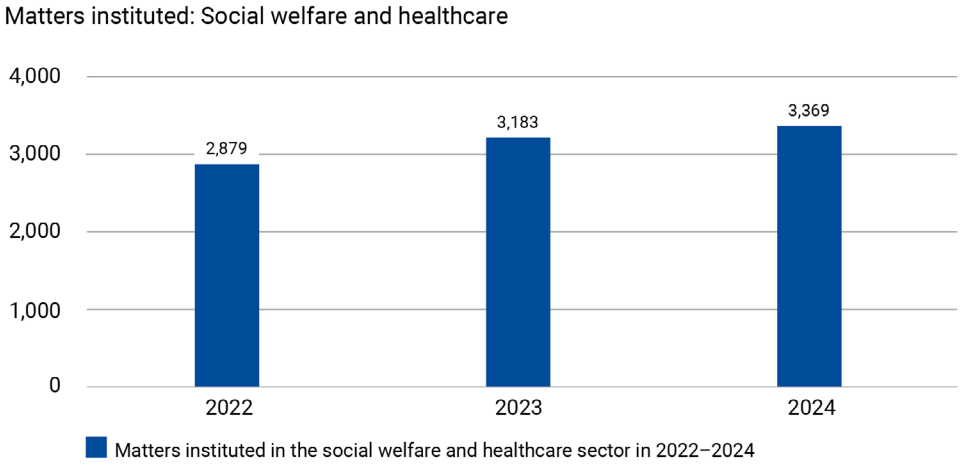
The number of clients and patients who contacted the Office of the Data Protection Ombudsman in cases related to accessing client or patient data without authorisation increased. In such situations, the person is instructed to request log data from the healthcare provider or a statement on the bases of data use or disclosure. In addition, the persons are instructed to report the crime to the police, which can then request a statement from the Office if needed.

People are interested in how their client or patient data is processed. The client or patient can request to be informed of who has used their data or to whom their data has been disclosed and the bases for these. The Court of Justice of the European Union (CJEU) issued a judgment in case C-579/21 in June 2023 that clarifies the right to access log data under the GDPR. According to the judgment, the right of access also grants data subjects the right to be informed of the times and purposes of the processing of their personal data. Under the Finnish act on the processing of social welfare and healthcare client data (*Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023*), data subjects also have the right to be informed of the bases for using or disclosing their data and an assessment of whether the use or disclosure of their data has been lawful. If this information is not provided, the case can be brought to the Office of the Data Protection Ombudsman, and the Data Protection Ombudsman can order the organisation to provide the information if necessary.

In the spring, the Deputy Data Protection Ombudsman issued a decision that concluded that patients' personal identity codes must not be included in text messages sent to patients automatically. A wellbeing services county was instructed to note the deficiencies in the security of sending information by text message and to also assess what information is required to be included in text messages related to laboratory tests, for example.

The legislation applicable in social welfare and healthcare will be amended in the near future as required by the European Health Data Space Regulation (EHDS). The Office of the Data Protection Ombudsman was part of the steering group for the national coordination related to the draft Regulation in 2024.





Education

During the year, the Office of the Data Protection Ombudsman provided several statements to the Ministry of Education and Culture, and the Finnish National Agency for Education. A statement was provided to the Finnish National Agency for Education on a draft guide on the use of AI applications in the processing of the personal data of children in early childhood education, and pupils and students. The statement highlighted the obligation of the education provider to find out before introducing any AI or other applications whether the application processes its users' personal data and to ensure that the processing is lawful. The hallucinations and biases of AI can also violate the fundamental rights of learners. The statement also highlighted that learners should be taught as a civic skill how AI applications process their users' personal data and what rights the users have.

An amendment was proposed to be made to the Act on Primary and Secondary Education (628/1998) that would allow using mobile phones during lessons only with permission from the teacher and for learning purposes, or for personal healthcare like diabetes management with permission from the principal or teacher. The Data Protection Ombudsman highlighted in the statement that education providers must ensure in advance that the applications they use in their teaching process the pupils' personal data lawfully. This also applies to free applications and applications using AI.

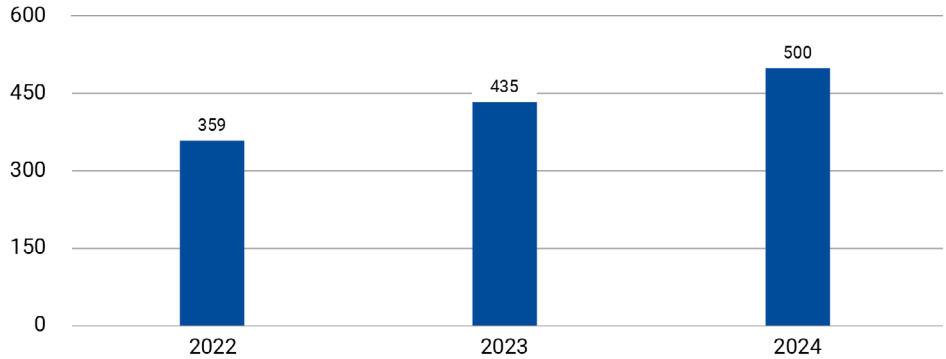
Revision of the provisions in the Act on Primary and Secondary Education pertaining to supporting learning and school attendance was also proposed. The Data Protection Ombudsman noted in the statement that the proposed legislation includes processing of sensitive and also classified data of children. It is important that the processing of such data is made uniform throughout Finland and that the necessary protective measures are also considered in the legislative drafting.

In the statement on the amendments to the Act on Early Childhood Education and Care (540/2018), the Data Protection Ombudsman also noted that personal data processing in early childhood education should be harmonised to safeguard the rights and freedoms of children. In addition, when the bases in the national early childhood education curriculum are reviewed, it is important to also discuss the processing of children's personal data.

In addition to data protection legislation, in the interdisciplinary cooperation of student welfare, the disclosure of pupil and student data is governed by sector-specific provisions that define the requirements and methods for data disclosure. In addition to educational authorities, the interdisciplinary cooperation comprises the psychologist and counselling services provided by social welfare and healthcare as well as school healthcare. The Deputy Data Protection Ombudsman submitted an initiative in 2022 to the Ministry of Education and Culture, the Ministry of Social Affairs and Health, the Finnish Institute for Health and Welfare and the Finnish National Agency for Education related to creating a guideline for the student welfare psychologist and counselling services on the disclosure of learners' personal data. The guidelines were drafted in 2023 and updated in 2024, and in addition to legislation, the guidelines affect the design of information systems, as the information is disclosed electronically.

In addition, the Deputy Data Protection Ombudsman provided a statement to the Ministry of Education and Culture on issues related to the data processing of the Move! system. Move! is a national system for measuring the physical fitness of pupils on the 5th and 8th grades and providing related feedback. The measurements are carried out as part of physical education.

Matters instituted: Education, early childhood education and care and youth work



Matters instituted in the field of education, early childhood education and care, and youth work in 2022–2024. Statistics on youth work have been compiled since 2024.

Judicial and security administration

The Data Protection Ombudsman supervises compliance with the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security in the activities of internal security authorities. The decision that the Deputy Data Protection Ombudsman issued in September pertained to the question whether the Police of Finland was allowed to collect personal identifying characteristics in its register in a case where a person was suspected of committing the basic form of defamation. The decision concluded that entering the personal identifying characteristics in the register violated the principle of proportionality laid down in the Coercive Measures Act (806/2011) and EU law, among other provisions. The Police of Finland was ordered to erase the personal identifying characteristics from its register. The decision is final. The decision was provided to the Ministry of Justice for its information and to enable assessing whether amendments are required to the Coercive Measures Act.

During 2024, the Office of the Data Protection Ombudsman issued several statements on judicial and security administration's legislative projects and other development projects. For example, the Data Protection Ombudsman provided a statement on the Government proposal for the amendment of the Aliens Act (301/2004) and the proposal to amend the Act on Military Intelligence (590/2019). The Office of the Data Protection Ombudsman also took part in the work of the Ministry of Justice's election security cooperation group.

In the autumn, during its Presidency of the Council of the EU, Hungary submitted a Presidency compromise proposal on the Regulation Proposal on Child Sexual Abuse Material (CSAM). The Office of the Data Protection Ombudsman addressed the Presidency compromise proposal in parliamentary committees in October 2024. The Data Protection Ombudsman considered that the proposed regulation continued to pose significant challenges as it would allow for the broad and indiscriminate scanning of private messages. The Data Protection Ombudsman had commented on the proposal earlier in October 2023. Even then, the opinion raised concerns about the disproportionate interference of the proposal in the protection of people's privacy and the powers held by authorities. In February 2024, the EDPB presented its views regarding the European Parliament's position on the proposed regulation. In its opinion, it welcomed many of the improvements proposed by Parliament, but stressed that they do not seem to fully resolve issues related to the general monitoring of private communications and the issuing of detection orders.

In November, the Supreme Administrative Court issued a decision on a decision of the Deputy Data Protection Ombudsman related to the Ministry for Foreign Affairs' compliance with the deadlines set for notifying personal data breaches. The Supreme Administrative Court upheld the decision insofar as it pertained to the delayed notification made to the supervisory authority and the remand issued for the delay. However, the Supreme Administrative Court repealed the Deputy Data Protection Ombudsman's decision insofar as it pertained to the delayed notification made to the data subject. The Supreme Administrative Court deemed that the Ministry for Foreign Affairs could be considered to have notified the victims of the data breach as required in the GDPR.

In June, the European Data Protection Board issued a guideline on data transfers under the EU Law Enforcement Directive. The guidelines provide guidance to the law enforcement authorities of EU countries in cases where they transfer data to the authorities of non-EU countries or international organisations.

One of the tasks of the Office of the Data Protection Ombudsman is to provide statements when requested by a prosecutor or a pre-trial investigation authority on four of the offences in chapter 38 of the Criminal Code: data protection offence, secrecy offence, unlawful access to an information system, and violation of the secrecy of communications. The purpose of the statements is to ensure a sufficient level of expertise in data protection matters in these offences that are less often brought to a consideration of charges.

In 2024, the number of statements issued grew significantly. A total of 110 statements were issued, when the number was 54 previously. Most of the statements were issued in cases involving a data protection offence. A data protection offence is committed when a person who has lawful access to a registry misuses the data. For example, if an employee or a public official views data without a legitimate basis, they commit a data protection offence. Most often, the unlawful data processing occurred in the information system of social welfare and healthcare services, but there were also cases where the unlawfully accessed information was in the register of the Police of Finland. Some of the statements were given in cases related to unlawful access to an information system and violations of the secrecy of communications. Most of these were related to gaining unlawful access to social media user accounts. Only a few statements were issued in cases involving a secrecy offence.

Other public administration

Practices in implementing the rights of data subjects were assessed in a decision issued to the Finnish Tax Administration in August, among other decisions. The Deputy Data Protection Ombudsman deemed that data protection legislation does not prevent data subjects from using their right through another person and a data subject can request access to their data through an attorney as well as request the organisation to deliver the data subject's data to the attorney. The Deputy Data Protection Ombudsman also reminded that there are no requirements for the format of an access request and that organisations must facilitate the making of access requests. However, they must still also ensure information security and find a balance between making the use of their rights easy for data subjects and implementing their rights in a secure way. The decision is final.

In December, the Deputy Data Protection Ombudsman deemed that the Finnish Tax Administration's Grey Economy Information Unit had the right to refuse to fulfil a person's data access request. The Unit was also not under any obligation to inform the person whether their data was processed at all in connection with a compliance report. The Finnish Tax Administration was also allowed to instruct the person to submit an access request to the authorities who are legally obligated to request a compliance report, which the Finnish Tax Administration listed for the person in its decision.

In 2024, a working group memorandum on updating the Act on the Openness of Government Activities (621/1999) was sent out for consultation. In the Data Protection Ombudsman's view, it is important to consider the right to privacy and data protection obligations when regulating the openness of government activities and document secrecy.

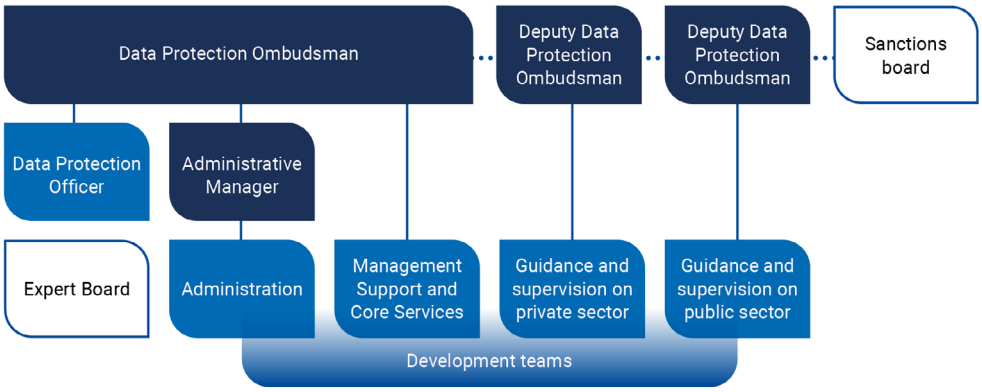
Organisation, personnel and finances

In 2024, the number of the Office of the Data Protection Ombudsman's employees increased from the previous year. At the end of the year, 60 people worked at the Office.

During the year, the organisational structure, which was reformed in the previous year, was further established. The purpose of the reform was to ensure smoother operations and increase job satisfaction. In autumn 2024, a development project was started with the aim of supplementing the measures taken in order to achieve the Office's objectives. Two sub-projects will focus on the work processes, the organisation of work, the work community and the work culture of the Office.

The Office's organisation comprises four units: private-sector guidance and supervision unit, public-sector guidance and supervision unit, administrative unit, and management support and core services unit. The administrative unit is responsible for the Office's administration, information management, registry services and management support. The core service unit is responsible for coordinating international cases and communications, and it comprises the Office's IT specialists, communications, senior specialist and the data protection officer.

Organisation structure of the Data Protection Ombudsman



The Data Protection Ombudsman is the head of the core services unit, the Deputy Data Protection Ombudsmen head the private-sector guidance and supervision unit and the public-sector guidance and supervision unit, and the Administrative Manager heads the administrative unit. The Office's two Team Managers serve as the closest supervisors of inspectors and legal specialists in the private-sector guidance and supervision unit and the public-sector guidance and supervision unit. The positions of the Team Managers were created in the 2023 organisation reform. Distributing managerial work to more persons than before has been found a good change.

Legal specialists, inspectors, senior inspectors and IT specialists process the data protection cases instituted at the Office. The legal specialists are responsible for cases requiring guidance and advice as well as tasks related to the screening procedures. Inspectors process cases that can be processed according to established practices. Senior inspectors are responsible for the most complex decisions and cases requiring guidance according to their areas of responsibility. They also draft statements on legislation, for example. IT specialists process technical personal data breaches in particular, and otherwise serve as experts in other supervision cases.

Separate development groups also coordinate certain subject matters, such as practices and projects related to data breaches, data subjects' rights and cross-border cases.

In 2023 and 2024, the Office of the Data Protection Ombudsman received additional appropriations to secure the performance of the Office's tasks and for the performance of certain new tasks arising from amendments made to legislation. The additional resources became fully apparent in the number of personnel in 2024, as new positions were created with the additional appropriations.

Human resources*	2022	2023	2024
Number of personnel at the end of the year	54	54	60
Person years	51.9	52.7	61.4
Absences due to illness, day(s) per person years	13.2	5.6	8.8
Average age	39.3	42.1	40.9
Education index	6.4	6.4	6.5

* Figures for 2022 and 2023 include the personnel of the Office of the Data Protection Ombudsman and the Office of the Intelligence Ombudsman (3–4 persons). The statistical method has been changed in 2024 to include only the personnel of the Office of the Data Protection Ombudsman. The Intelligence Ombudsman shared administrative functions with the Office of the Data Protection Ombudsman until the end of 2024.

Finances of the Office of the Data Protection Ombudsman	Realisation 2022	Realisation 2023	Target 2024	Realisation 2024
Use of the operating expenses appropriation, €1,000	4,041	4,324	6,050	4,991
Total costs, €1,000	4,450	4,730	-	5,853

Guidance and communications

– fulfilling information needs

The Office of the Data Protection Ombudsman's telephone guidance service provides general guidance on data protection and personal data processing. The service has two telephone numbers, one for private individuals and one for controllers and data protection officers. The guidance provided is general and no detailed or binding statements will be provided for individual cases.

In June 2024, the telephone service introduced a queueing function that allows a caller to stay on the line to wait for their turn if the line is busy. The queueing function improved the accessibility of the service and reduced the number of calls received. Compared to the previous year, 2024 was a quieter year for the telephone service and the number of calls answered reduced to around 2,300. The line for private individuals was again busier that the line for controllers. General guidance is also provided in writing and during the year, around 1,230 guidance requests were responded to.

Guidance was extensively provided on data subjects' rights, requests related to them and the practical implementation of the requests. Among the most common questions were those pertaining to whether email messages or other unofficial files or notes are also covered by the right of access. For the part of social welfare and healthcare, questions on log data were still regular.

As in previous years, many of the contacts were related to unlawful access to an information system and personal data breaches. Controllers requested guidance on how the definition of a personal data breach should be interpreted and on what to do in the event of a breach. The larger personal data breaches seen, such as the City of Helsinki data breach, resulted in a large number of contacts in particular.

Video surveillance was a subject in questions from both private individuals and controllers. The questions were related to the legal bases of video surveillance and processing of the recordings, for example. Some were related to real-time video surveillance. Questions on data protection in working life included topics such as work email, processing of location data and situations where an employee is expected to use their private phone or online banking credentials in work tasks. Some questions pertained to whether the GDPR also applies to oral discussions had during a coffee break.

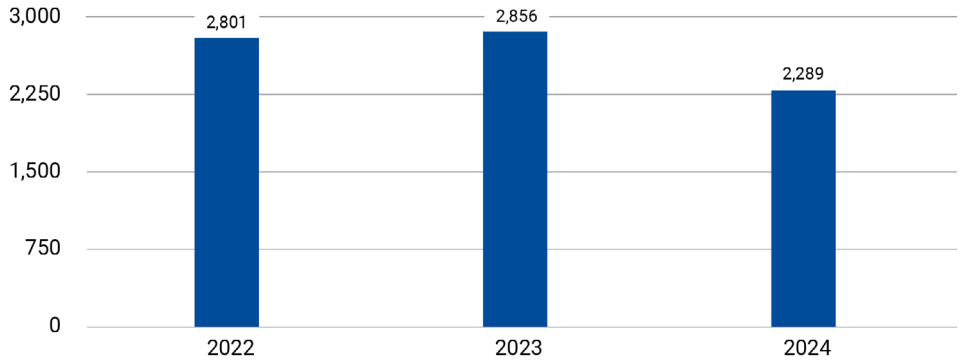
General information on personal data processing related to the Positive credit register, which was launched in April, was comprised to the Office of the Data Protection Ombudsman's website. Updated instructions for organisations and managers that have appointed a data protection officer were also published on the website. The most frequent questions asked related to healthcare were updated, among other things, for the part of accessing client and patient information, and requesting their correction or erasure.

Information on the EU's Digital Service Act (DSA) and the Data Protection Ombudsman's authority in the related monitoring was also published on the website. The DSA became applicable in February, and it introduced new responsibilities for online platforms and other digital services.

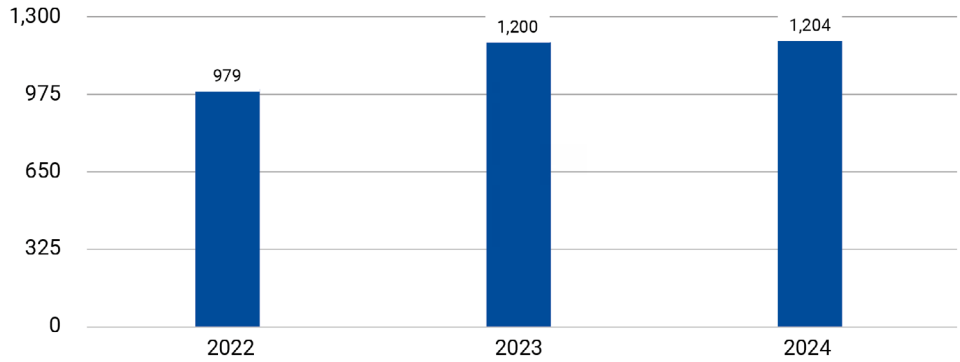
In the summer, the new website Data protection in hobbies (Tietosuojaharrastuksissa.fi) was launched in collaboration with the TIEKE Finnish Information Society Development Centre. The website was created as part of the 'GDPR4CHLDRN – Ensuring data protection in hobbies' project.

The Office of the Data Protection Ombudsman takes part in training data protection officers and other data protection professionals. In January 2024, the Office organised an event on the international Data Protection Day for the fifth time in collaboration with Alma Insights. Nearer to the end of the year, the social welfare and healthcare SohviTellu seminar was organised in Hämeenlinna in collaboration with operators in the sector.

Answered phone calls in the telephone guidance service



Data Protection Ombudsman in the media (references in online media)



Matters instituted and processed in 2022–2024

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 2022–2024. 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.

	2022		2023		2024	
	Instituted	Resolved	Instituted	Resolved	Instituted	Resolved
Tasks in accordance with the GDPR and the Data Protection Law Enforcement Directive						
Prior consultation (high risk)	71	249	23	25	11	8
Statements	408	417	287	301	160	145
Statements in criminal cases*					98	110
Codes of Conduct	0	1	0	2	0	1
Transfers of personal data	26	18	3	18	7	57
EU and international cooperation	1,018	1,016	1,362	1,297	1,390	1,131
Rights of the data subject	834	950	838	994	797	819
Supervision	1,063	1,069	1,268	1,197	1,276	1,173
Personal data breaches	5,446	5,663	6,894	6,487	7,152	7,467
Guidance and advice	1,176	1,441	1,318	1,592	1,209	1,247
Data Protection Officers	255	269	267	260	473	459
Board of Experts	2	2	2	2	1	1
General, financial and human resource issues	796	774	917	884	710	673
Total	11,095	11,869	13,179	13,059	13,284	13,291

*Separate statistics since 2024

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