OFFICE OF
THE DATA PROTECTION OMBUDSMAN

ANNUAL REPORT
OF THE OFFICE OF THE DATA PROTECTION OMBUDSMAN OF FINLAND 2025

ANNUAL REPORT

OF THE OFFICE OF THE DATA PROTECTION OMBUDSMAN OF FINLAND 2025

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).

Anu Talus served as the Data Protection Ombudsman in 2025. In June 2025, the Ministry of Justice appointed Talus to the post of Data Protection Ombudsman for the next term of office starting on 1 November 2025. The Deputy Data Protection Ombudsmen were Heljä-Tuulia Pihamaa and Annina Hautala.

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:

Transformations are shaping the operating environment

The data protection environment is currently being shaped by the geopolitical situation, legislative reform and the debate on the EU's competitiveness. The duties of the data protection authority are also expanding.

In 2025, the Office of the Data Protection Ombudsman was granted additional resources for the performance of statutory duties. A plan for a new organisational structure was finalised and a four-stage recruitment plan drawn up during the year. It was decided to establish a total of five areas of responsibility based on the Office's private and public sector guidance and enforcement units. An EU and international affairs team and IT-focused team were established in the Management Support and Core Services Unit. The new teams are led by team leaders. At the same time, we started creating structures for the new enforcement duties that the Office of the Data Protection Ombudsman will be assigned, especially under the EU AI Act.

In the public debate on data protection, events in world politics have brought digital sovereignty to the fore in a new way. It is a question of who ultimately controls and has access to data in the digital environment. These are also significant issues in data protection regulation and international data transfers.

Transfers of personal data, particularly to China, became a subject of debate during the year. The Data Protection Ombudsman began an investigation into a university's data transfers to a Chinese company. The Irish data protection authority also imposed an administrative fine of EUR 530 million on TikTok for the unlawful transfer of personal data to China. The decision was made in a cooperation procedure between the European data protection authorities, in which the Data Protection Ombudsman participated. This procedure involves the preparation of a joint decision that is binding on all supervisory authorities.

We participate in the processing of approximately 500 cross-border matters each year. A new EU regulation, which harmonises and expedites the activities of data protection authorities in matters involving several Member States, will affect the processing of complaints from April 2027 onwards.

In addition to digital sovereignty, the EU's competitiveness has taken centre stage in the public debate. The Draghi report published in 2024 identified difficult, multi-layered digital regulation as one of the factors undermining competitiveness. The European Commission has proposed a number of reforms aimed at streamlining regulation. The proposed amendments to the GDPR appear to be largely in line with the established interpretations of European data protection authorities. However, the definition of personal data proposed in the so-called Digital Omnibus proposal has raised concerns, as it would differ from the established practice of the European Court of Justice and create uncertainty about the interpretation of the concept of personal data.

The heads of the European data protection authorities met at a high-level meeting of the European Data Protection Board in Helsinki in July 2025. The Helsinki Declaration was issued at the meeting, in which we committed to providing concrete support to organisations and ensuring the most uniform application practice possible in the EU. The main objective is "*GDPR made easy*". At the same time, closer cooperation with authorities and stakeholders in other fields was agreed upon.

Extending the powers of the authorities has been a strong trend in both national and European legislative projects, and several statements on the proposed changes to the authorities' right of access to information were requested from the Data Protection Ombudsman in 2025. The legislative reforms have important aims, such as combating crime and the grey economy. However, the amendments must be proportionate and necessary and the powers of the authorities precisely defined. One of the legislative reforms would extend the Tax Administration's right to receive information on the bank transactions of Finnish citizens. In its statement, the Constitutional Law Committee of Parliament required changes to the proposal.

Parliament also discussed the Government's position on the EU CSAM Regulation, which combats online sexual violence against children.

In the public debate on data protection, events in world politics have brought digital sovereignty to the fore in a new way.

Finland and several other Member States opposed the mandatory decrypting of secure connections in communications applications. Other major legislative projects included proposals for amendments to data protection legislation and the system of sanctions provided therein.

As the operating environment becomes more complex, there is an increasing need for cooperation between authorities at both national and European levels. The rapid development of technology and regulation will only increase the need to safeguard the fundamental rights of people.

Anu Talus
Data Protection Ombudsman

Deputy Data Protection Ombudsman Heljä-Tuulia Pihamaa:

The data protection year was characterised by artificial intelligence and secure data processing

The year 2025 was characterised by the rapid adoption of AI, especially in the private sector. Companies deployed different kinds of AI tools at an accelerating pace and AI-related questions emerged as one of the key themes of the year. The national acts concerning the EU's AI Act entered into force on 1 January 2026, and at the Office of the Data Protection Ombudsman we started preparations for our new authority tasks. As part of our preparations, we published guidelines on how to take data protection into account in AI systems. This work will continue actively in 2026.

Developing sustainable and ethical AI requires close cooperation both at the national as well as the international level. AI was also the main theme in the annual Global Privacy Assembly, which emphasised the significance of data protection regulations and especially data protection principles in the development of AI and the need for cooperation between authorities. In Finland, the cooperation building process started among 15 national authorities supervising AI under the coordination of the Finnish Transport and Communications Agency Traficom.

AI adoption was also reflected in data breach notifications. In several cases, the risks related to the processing of personal data were not sufficiently assessed before the introduction of new tools. This highlights the controller's obligation to pay attention to data protection already at the planning phase.

Data breach notifications continue to be the largest case group at our Office. During the year, we continued with our project that aimed at the utilisation of automation in the processing of notifications. Our goal is to introduce automation during 2026.

In 2025, the Office of the Data Protection Ombudsman's sanctions board imposed three administrative fines for data protection violations.

These decisions shared a common theme of the secure processing of personal data in industries in which the processing of personal data is part of the organisations' core operations and the processed data is sensitive. Careful management of change processes and pre-testing of information systems were emphasised in the decisions. After all, many data protection risks are still associated with the deficiencies in operating methods and not solely with technical challenges. Planning, caution and proactive assessment regarding the processing of personal data cannot be overemphasised.

We also received several significant precedents from the Supreme Administrative Court, especially in the insurance sector. The Supreme Administrative Court set a precedent in the interpretation of the concept of an insured person as well as the prerequisites for a request for information which insurance companies submit for health care in order to settle claims. The precedents ruled against the Data Protection Ombudsman's positions. At the same time, they highlighted that the insurance companies' requests for information must be justified, specified and necessary. We have emphasised in various contexts that the processing must also be predictable and transparent for the customer.

In June, the Supreme Administrative Court issued a significant precedent in the access rights of user log data in the so-called S-Bank case. Customers had the right to access the purposes and dates of the processing, but not the identity of the employees who processed the data. Access rights regarding log data was also reflected in the advice requests received by the Office.

At the EU level, debate was sparked by the supervision of the Digital Services Act (DSA), age verification of online services and the protection of children on online platforms. The close supervisory cooperation of the DSA, led by Traficom, continues, and growth was also seen in the supervisory cases. At the end of the year, the first decisions concerning tech giants were issued by the European Commission, when the first-ever fine regarding non-compliance with the transparency obligations under the DSA was issued to the social media service X.

Developing sustainable and ethical AI requires close cooperation both at the national as well as the international level.

As in previous years, questions regarding the rights of data subjects were strongly present in guidance and supervision. The right to erasure of personal data was under review when the authorities of the EU and ETA countries clarified the practices and challenges of organisations in the realisation of the right. It is even more critical to safeguard strong data protection rights now that data collection in the digital environment is changing and constantly increasing due to new technologies.

Heljä-Tuulia Pihamaa
Deputy Data Protection Ombudsman

Deputy Data Protection Ombudsman Annina Hautala:

Comprehensive security requires strong data protection

To put it dramatically, the current difficulties facing the world have been reflected in the activities of the Data Protection Ombudsman. New threat scenarios have emerged in the implementation of data protection. At the same time, it could be stated that the changes in the operating environment have been as expected. The world has continued to become more complex, personal data processing has increased and technology, especially AI, has continued to evolve and normalise.

Data protection plays a crucial role in democracy, social stability and enhancing security. After all, data protection is a significant part of comprehensive security. Society's approach to privacy and data protection has a direct impact on how society remains democratic and secure. In this, public sector operators play a key role. The fundamental aspect of the Office of the Data Protection Ombudsman's work is guidance and supervision of the processing of personal data by the state, municipalities and wellbeing services counties. This year, we have taken a stand on, for example, whether children's biometric data can be processed for a certain purpose in the education sector and launched an investigation into the transfer of genetic information to a Chinese company.

In the midst of all these changes, it is important that organisations and individuals are aware of which personal data is processed through technological means at a given time and for which purposes, as well as that the management and decision-making power related to the data is not intentionally assigned elsewhere; for example, to large technology companies. It should not be forgotten that the framework created by the data protection legislation concerns the processing of personal data regardless of the technology used.

As in previous years, the majority of cases were initiated in the healthcare and social welfare sector. Approximately one quarter of the initiated cases concerned this sector. A large proportion of cases regarding the public administration were related to personal data breaches and to the exercise of individuals' data protection rights. The general advice for data subjects is to first contact the organisation processing their personal data when they wish to exercise their data protection rights.

Many personal data breaches were typically caused by human error. It is also evident that in many cases the reason behind the personal data breach was old and out-of-date equipment and systems, as

well as other deficiencies in information security. I want to emphasise that everyone should pay attention to good information management and the supervision of the processing of data, as well as delete unnecessary data in order to minimise any damage.

One important part of our work is to support legislative drafting. This year, we drew the legislator's attention several times to the impacts of the expansion of the right of access to data by the authorities and their processing rights, deficiencies in the impact assessment of data protection, clarity of responsibilities and the balance related to the fulfilment of basic rights. During the year, we provided statements regarding, for example, the government proposal on the Tax Administration's right of access and a proposal which aims to expand the possibility to utilize the biometric data stored in the passport registers of the police in criminal investigations. We also provided multiple statements concerning early childhood education and the education sector, as well as the healthcare and social welfare sector.

During the year, our Office delivered more than a hundred statements supporting the consideration of charges. It is worth noting that a significant proportion of these statements concerned suspicions of unauthorised access. We have also been handling exceptionally extensive unauthorised access cases.

Proactive guidance is the core task of the Data Protection Ombudsman. When the number of written guidance and advice requests is combined with telephone advice cases, the total number of requests handled amounts to nearly 4,000 during the year. In our everyday work, we try to find the balance in how detailed advice we, as the supervisory authority, can offer in advance. During the year, we carried out several audits among controllers, and during which we could provide assistance in the data protection work of organisations.

The approach to privacy and data protection has a direct impact on how society remains democratic and secure.

We engaged in stakeholder cooperation in various different ways. For example, we participated in project of the Association of Finnish Cities and Municipalities and also in the VAHTI activities promoting cyber and digital security.

Despite the changes taking place around us and our busy work schedule, it has been a pleasure to see how our personnel have again this year persistently worked with a high level of professionalism when it comes to data protection. In addition to our skilled employees, the independence of the supervisory authority, functional processes and sufficient resources are prerequisites for succeeding in this work.

Annina Hautala
Deputy Data Protection Ombudsman

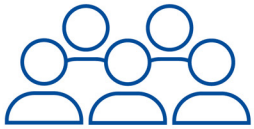
Office of the Data Protection Ombudsman's year 2025 in figures

15,408

Cases instituted

15,033

Cases processed



64

Number of personnel at end of year

In 2025, the Office of the Data Protection Ombudsman issued

3 decisions imposing administrative fines for data protection violations

30 reprimands for processing measures that violated data protection legislation

8 orders to bring personal data processing measures into compliance with the GDPR

8 orders to fulfill the rights of the data subject

4 orders to notify data subjects about a personal data breach

3.765

Total administrative fines (million euros)

7,355

Personal data breach notifications

10

Audits initiated or carried out

2,579

Calls answered by the telephone service

39

Statements on legislative projects

100

Statements to prosecutors and pre-trial investigation authorities

22

Lead supervisory authority in cross-border cases

484

Supervisory authority concerned in cross-border cases

Events in 2025

JANUARY

- Investigation into a data breach of Valio's information network began
- EDPB published a guideline on the pseudonymisation of personal data
- The report on an European investigation on the right of access was completed
- The Data Protection Day event was held for the sixth time in Helsinki

FEBRUARY

- The Supreme Administrative Court enforced the Data Protection Ombudsman's decision on tax information portals
- The prohibitions laid out in the EU AI Act entered into force
- The EDPB created a task force on AI enforcement
- The Data Protection Ombudsman issued a statement on a legislative amendment extending the rights of the police to access information

MARCH

- A European investigation on the right to erasure of personal data was launched
- The Data Protection Ombudsman commented on the assessment of creditworthiness on the basis of sufficient information
- Persons involved in county and municipal election campaigns were reminded of data protection
- An investigation into data transfers by the University of Helsinki to a Chinese gene technology company was started
- The EHDS Regulation entered into force

APRIL

- Finland's first BCRs were adopted

MAY

- Yliopiston Apteekki was fined for data protection shortcomings in its online pharmacy's tracking technologies
- The data protection authorities of the Nordics met on the Faroe Islands
- EU data protection authorities imposed an administrative fine on TikTok for illegal transfers of personal data to China

JUNE

- The Deputy Data Protection Ombudsman issued a decision on information to be provided in connection with telemarketing
- The Supreme Administrative Court issued a precedent on the right of access to log data

JULY

- A high-level meeting of EU data protection authorities took place in Helsinki
- Data protection authorities launched a new investigation into TikTok

AUGUST

- The Data Protection Ombudsman issued a statement on the proposal to amend the Act on Taxation Procedure

SEPTEMBER

- An administrative fine was imposed on S-Pankki for a security vulnerability in its mobile service
- Application of the EU Data Act began
- In its decision, the Court of Justice of the European Union clarified the processing of pseudonymised data
- The EU–US data privacy framework was upheld by a decision of the General Court of the EU
- The EDPB issued a guideline on the relationship between the GDPR and DSA
- The main item on the agenda of the Global Privacy Assembly was AI

OCTOBER

- An administrative fine was imposed on Aktia for security shortcomings in its strong electronic authentication service
- The investigation by the Office of the Data Protection Ombudsman on the use of cloud services in central government was completed
- The online form for reporting data breaches was overhauled
- The Data Protection Ombudsman commented on amendments related to the overall reform of data protection legislation
- Application of the EU regulation on the transparency and targeting of political advertising began
- The EDPB and Commission issued a joint guideline on the relationship between the GDPR and DMA

NOVEMBER

- The Commission published the Digital Omnibus proposal
- Anu Talus began her second five-year term as Data Protection Ombudsman
- The Data Protection Ombudsman issued a statement on the bill for the imposition of administrative fines in the public sector
- A regulation on cross-border processing supplementing the EU General Data Protection Regulation was adopted

DECEMBER

- A national Act on the Enforcement of the Artificial Intelligence Regulation was adopted
- The Supreme Administrative Court issued a precedent on the processing of the health data of an insurance applicant
- The EDPB published recommendations on requiring a customer to create an account in online shops

Focus areas of data protection work

Overview of statistics and the field

Number of cases grew significantly

The number of cases instituted with and processed by the Office of the Data Protection Ombudsman increased significantly compared to the previous year. A record number of 15,408 cases was instituted in 2025. This represented an increase of 2,100 from the previous year. A total of 15,033 cases were processed, which is over 1,700 more than in the previous year.

A significant part of the increase was explained by the exceptionally high number of Data Protection Officer declarations. One of the statutory duties of the Office of the Data Protection Ombudsman is to maintain a list of organisations' data protection officers. The list was updated in 2025, due to which more than 900 declarations were received, which is hundreds more than usual.

Personal data breach notifications are the largest category of cases at the Office of the Data Protection Ombudsman, and their number has been increasing each year. A total of 7,355 data breaches were reported during the year, constituting an increase of 200 notifications from the previous year. However, the relative share of notifications among instituted cases declined.

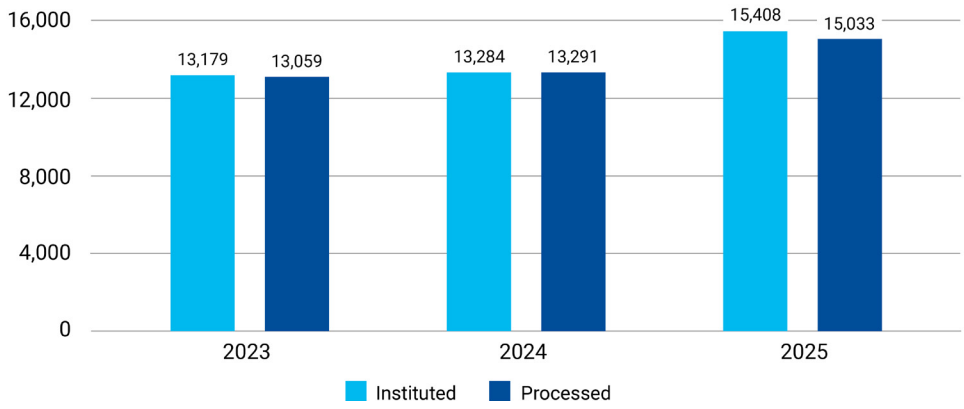
Other major case categories include tasks related to enforcement, guidance and counselling, EU cooperation, and complaints and requests from private individuals.

Since the beginning of 2024, the Office of the Data Protection Ombudsman has been obliged to decide on a complaint or to notify the person of an estimated decision date within three months of the institution of the case. A person may appeal to the administrative court about the inactivity of the data protection authority if it does not comply with this deadline. Most cases are decided before the deadline. Approximately 4,260 cases subject to this recourse were instituted in 2025. More than 860 complaints and about 1,120 requests concerning data protection rights were received from private individuals. These numbers increased by several hundreds from the previous year.

Approximately 1,450 cases instituted in 2018–2023 that were over two years old were unresolved at the end of 2025. At the end of 2024, the corresponding number was 1,200 cases. Cases processed in cross-border cooperation, where the procedure is led by a supervisory authority of another EEA country, constitute a significant proportion of old cases.

Under the Whistleblower Protection Act, the Office of the Data Protection Ombudsman is the competent supervisory authority for notifications concerning the protection of privacy and personal data as well as the security of network and information systems. It must report the number of notifications made under the Whistleblower Protection Act annually to the Chancellor of Justice. The Office of the Data Protection Ombudsman received eight new notifications in 2025. The processing and assessment of the notifications will continue in 2026.

Matters instituted and processed from 2023 to 2025



Transformations in the operating and regulatory environments

The transformations of the digital environment and global data economy shape the operating environment of the Data Protection Authority. New duties arising from digital and data regulation will broaden the enforcement responsibilities of the data protection authority, and the duties are only expected to increase further. National legislation is also being reformed.

As part of the overall reform of data protection legislation, preparations for amendments to the legislation under the administrative branch of the Ministry of Justice were launched in spring 2025. The reform proposes amendments to the Data Protection Act and ten other acts. In October, the Data Protection Ombudsman issued a statement on the draft government proposal. Among other things, the legislative amendments concern the mobility of information between authorities, the processing of sensitive personal data, and electronic data disclosure methods. Transferring the duty of accrediting the certification body from the Data Protection Ombudsman to the national accreditation body (FINAS) is also proposed. The acts are due to enter into force in September 2026.

The acts regulating violations of AI legislation and the powers of the national authorities enforcing the EU AI Act were adopted in December 2025 and entered into force on 1 January 2026. The enforcement of the AI Act has been decentralised to 15 different authorities in Finland. The Finnish Transport and Communications Agency Traficom serves as the national contact point. During the year, preparations were made for the start of the application of the AI Act in close cooperation by the authorities. The cooperation is coordinated by Traficom.

The Data Protection Ombudsman is one of the market surveillance authorities for high-risk AI systems, which monitor that the systems are lawful and there are no dangerous or unsafe products on the EU single market. The Data Protection Ombudsman also serves as a notified body for some high-risk AI systems. Upon request, the Ombudsman checks the compliance of AI systems designed for use by certain security authorities before their adoption. The Data Protection Ombudsman enforces the prohibitions of the AI Act and serves as the data protection authority and supervisory authority for fundamental rights. The prohibitions of the most harmful AI use cases started to apply in February 2025.

The application of the EU Data Act (DA) largely began on 12 September 2025, and the relevant national legislation entered into force in December 2025. The DA provides for the sharing of data generated by devices and services connected to the network and for the user's right to data. The Data Protection Ombudsman enforces compliance with the DA with regard to the protection of personal data. If an authority or other public actor requests data containing personal data from a company in a public emergency, the Data Protection Ombudsman must be notified of this.

The EU Digital Services Act (DSA) increases the security of online platforms and improves the position of digital service users. In Finland, the DSA is mainly enforced by Traficom. In 2025, the Data Protection Ombudsman was responsible for supervising the recognisability of political advertising, the transparency of online advertising and recommendation systems, and the protection of minors on online platforms.

The supervisory role of the Data Protection Ombudsman was changed as of 2026, when the amendment to the Act on the Supervision of Online Intermediation Services transferred supervisory tasks related to the transparency of social and political advertising to the National Audit Office. Going forward, the Data Protection Ombudsman will continue to supervise business-to-business advertising.

Close cooperation in the enforcement of the Digital Services Act continued in 2025. The number of enforcement cases processed by the national supervisory authorities increased from the previous year. The Data Protection Ombudsman received seven complaints in total. The Office of the Data Protection Ombudsman participated in the European Board for Digital Services' working group on the protection of minors with Traficom and met with representatives of the European Commission. In December, the European Commission adopted the first decisions on compliance with the Digital Services Act. The Commission is responsible for the supervision of very large online platforms.

The application of Regulation (EU) 2024/900 on the transparency and targeting of political advertising began in October 2025. The Regulation increases the transparency of political advertising and combats disinformation and foreign interference in elections. At the same time, it ensures that the targeting of advertising does not violate the protection of personal data. The Data Protection Ombudsman supervises the targeting and delivery of online political advertising when it involves the processing of personal data. National legislation supplementing the Regulation entered into force on 1 January 2026.

The transformations of the digital environment and global data economy shape the operating environment of the Data Protection Authority.

In December 2025, the EU adopted the new Regulation (EU) 2025/2518 laying down additional procedural rules on the enforcement of the GDPR. Application of the new Regulation will begin in April 2027. The Regulation enhances the functioning of data protection authorities in enforcement matters connected to more than one country in the European Economic Area. It provides for, inter alia, time limits, stages of investigation, the exchange of information between authorities and the rights of parties. The Office of the Data Protection Ombudsman has begun preparing for these obligations.

The European Commission aims to simplify EU regulation by means of omnibus legislative proposals. The Digital Omnibus and AI Omnibus proposals were submitted in November 2025. The Commission aims to facilitate compliance with regulations, improve Europe's ability to compete and reduce the administrative burden on businesses.

Personal data breaches

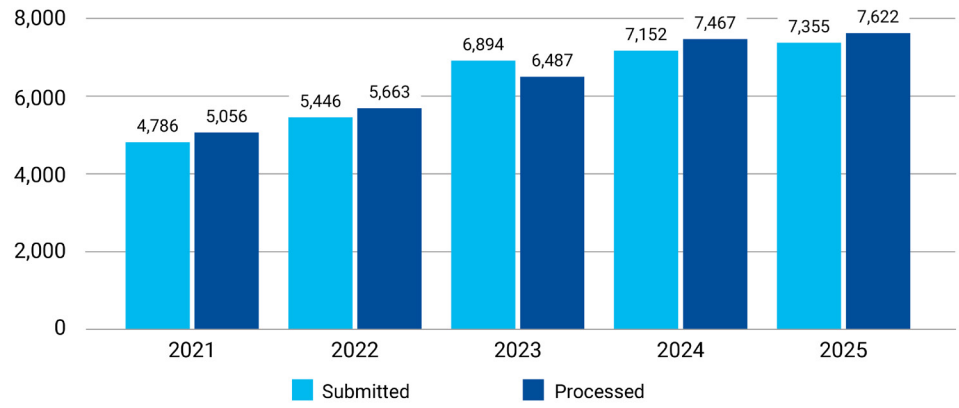
An organisation must notify a personal data breach to the data protection authority if the breach may pose a risk to the persons involved. The notification must be made without undue delay and not later than 72 hours after having become aware of the breach. The Office of the Data Protection Ombudsman can take action based on the personal data breach notification if necessary. Most notifications do not require further investigation or other follow-up measures, but especially large-scale data breaches often require more detailed investigation.

In 2025, approximately 7,350 data breaches were notified to the Office of the Data Protection Ombudsman and over 7,620 were resolved. The number of notifications received was approximately 200 more than in the previous year. The number of notifications corresponds to our European reference countries.

The annual increase in the number of notifications is probably explained by the general increase in digitalisation, IT development and increased awareness of the notification obligation among organisations. Since the application of the GDPR began in May 2018, more than 40,000 data breaches have been notified to the Office of the Data Protection Ombudsman. The largest number of notifications are received from regulated sectors, such as social welfare and health care and the financial sector.

Case flow management was a key focus of operations in 2025. The Office continued a development project aimed at streamlining the processing of data breach notifications and promoting the efficient allocation of authorities' resources. In autumn 2025, updates were made to the online form, which organisations use to notify data breaches in accordance with their

Personal data breach notifications



Submitted and processed personal data breach notifications in 2021–2025

notification obligation. The changes clarified the structure of the form and the wording of the questions. The instructions were also improved to make it easier to fill in the notification. The information notified with the form is now in a more structured format to make the processing of notifications more efficient and enable automated processing in the future.

Based on the notifications received, human error is the most common cause of data breaches. Examples of such cases include personal data becoming available to third parties or too widely or being accidentally disclosed to the wrong recipient, documents containing personal data being lost, or data being recorded incorrectly or for the wrong person. Phishing, i.e. unjustified data processing, is also a personal data breach that an organisation must notify to the Office of the Data Protection Ombudsman.

The year 2025 was marked by email phishing by which the attacker gained possession of the M365 account of an organisation's employee. The stolen credentials can give the attacker access to the user's email and other services in the M365 environment. In practice, M365 data breaches always target personal data as well. Adversary-in-the-middle (AiTM) technology, which bypasses multi-factor authentication, is also often used in phishing. The number of data breaches using AiTM technology increased towards the end of the year.

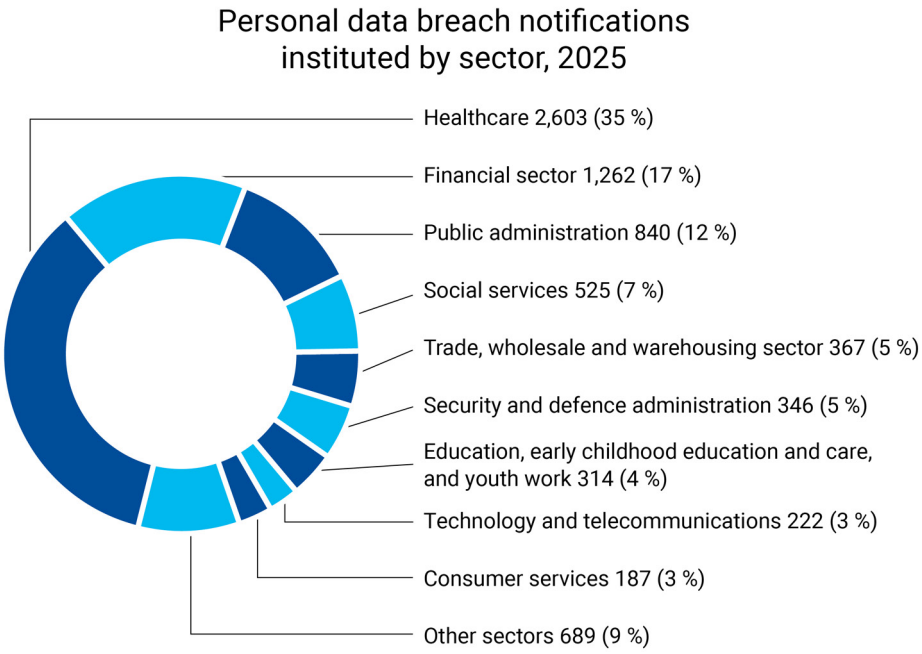
Attacks carried out with ransomware are also regularly notified to the Office of the Data Protection Ombudsman. In these cases, the data breach has usually been triggered by an edge device, such as a firewall or remote VPN connection device, or by a server that was unintentionally visible in the public network. The root cause of the breaches is usually a technical vulnerability, an incorrect configuration, leaked IDs or an unupdated device. Malware attacks are always serious.

The year 2025 was marked by email phishing.

Data breaches related to AI tools have been identified as a new phenomenon. Careful risk assessment is essential before the deployment of AI services.

Old and unupdated hardware and systems as well as inadequate information security make an organisation particularly vulnerable to technical security breaches. Vulnerabilities in unupdated devices and zero-day vulnerabilities are being exploited ever more rapidly. Data breaches can often be prevented by adequate technical safeguards, change process management, regular testing, access management and ensuring data protection competence. Minimising the amount of personal data processed and stored and good data management limit the damage.

In June 2025, an investigation team established in connection with Safety Investigation Authority Finland (OTKES) published an investigation report on the data breach against the City of Helsinki in spring 2024. The report issued recommendations for improving preparedness in the public sector and the prevention of cybercrimes. These recommendations included the development of communications guidelines, coordination of information management, supervision and the issuing of guidelines, and improving the detection of information security shortcomings in the public administration. The Office of the Data Protection Ombudsman continues to investigate the data breach from the perspective of compliance with data protection legislation.



European cooperation

The Office of the Data Protection Ombudsman is an active member of the European Data Protection Board (EDPB) and its subgroups. In the EDPB, the Office participates in the preparation of guidance, policies and opinions as well as in joint European decision-making. The EDPB consists of the national data protection authorities of EU and EEA member states and representatives of the European Data Protection Supervisor (EDPS). Data Protection Ombudsman Anu Talus is the Chair of the EDPB for the term 2023–2028.

In July 2025, the EDPB held a high-level meeting in Helsinki to agree on common policies for future work. In the Helsinki Declaration, European data protection authorities committed to new measures to facilitate compliance with data protection regulation in organisations of all sizes, to increase dialogue with stakeholders and to develop cooperation between authorities in different fields. For example, practical tools, lists and templates, such as for data breach notifications and data protection impact assessments, will be created to support organisations. In addition, the measures agreed in the declaration will further harmonise the application and interpretation of the GDPR in different countries.

In May 2025, the European Commission proposed amendments to certain provisions of the GDPR to simplify the requirements for small and medium-sized enterprises. In July, the EDPB and the EDPS issued an opinion on the proposal, stating that they would support targeted regulatory changes and the lightening of obligations for SMEs.

European data protection authorities committed to new measures to facilitate compliance with data protection regulation in organisations of all sizes.

In November, the Commission adopted omnibus proposals to simplify digital and data regulation and AI rules and requested an opinion on them from the EDPB and EDPS. The Digital Omnibus and AI Omnibus proposals propose changes to the GDPR, AI Act and other key data regulation in the EU.

Data protection authorities assessed the proposals' impact, in particular on compliance with regulations, legal certainty and fundamental rights. While the Commission's objectives and many regulatory changes are welcome, at the same time some of the proposed amendments to data protection regulation raise concerns. The proposed changes would narrow down the concept of personal data and delegate powers to the Commission in relation to the definition of personal data, which could lead to a deterioration in data protection.

The Commission has justified the proposed amendments to the concept of personal data by ruling C 413/23 P (EDPS v SRB) issued by the Court of Justice of the European Union in September 2025, which specified the interpretation of pseudonymised data. In the past, the Court has also issued other decisions addressing questions related to the identifiability of personal data.

Pseudonymisation means the processing of personal data so that it can no longer be linked to a specific person without additional information. The Court found that pseudonymised data may no longer be personal data if the processing organisation does not have reasonably likely means of returning the data to an identifiable form. Whether pseudonymised data continue to be personal data must always be assessed from the perspective of each organisation processing the data.

Issues related to the pseudonymisation of personal data were very much present in the Office's EU-level work during the year. Following the Court's ruling, the EDPB collected stakeholders' views and comments on questions of anonymisation and pseudonymisation. Based on these, the EDPB will update its guideline on pseudonymisation, which was published in early 2025. Guidelines are also being drawn up on the anonymisation of personal data.

The draft guidelines issued by the EDPB in 2025 dealt with the parallel application of the GDPR and Digital Services Act, among other things. The EDPB and the Commission drew up a joint guideline on the interfaces between data protection regulation and the EU Digital Markets Acts. Recommendations were issued for anti-doping activities and situations in which online shops may require the creation of a customer account. The EDPB set up an AI-focused task force to promote cooperation in the supervision of AI applications and the exchange of information between DPAs.

The protection of minors in digital services was a key theme. In February, the EDPB issued an opinion on age-limit control in digital services. The aim is to ensure a harmonised European approach to verifying age in order to protect children and young people online, while respecting data protection principles. In July, the European Commission published a prototype of the age verification application for online services and a guide on the protection of minors for online platforms.

The Nordic data protection authorities continued their close cooperation. The annual Nordic meeting was held in May, focusing on the supervision of AI solutions, information security issues and the efficient handling of matters in an increasingly complex data protection environment.

At the Global Privacy Assembly held in September, the Office of the Data Protection Ombudsman signed a joint declaration with the data protection authorities of twenty countries and regions, setting down their commitment to promoting innovative and responsible AI development.

Cross-border cases

Where personal data are processed in more than one Member State or the processing affects persons in more than one EU country, it constitutes cross-border processing of personal data. In that case, the data protection authorities of the EEA supervise the activities of organisations in cooperation. A lead supervisory authority, which cooperates with the supervisory authorities concerned, is identified for the case.

The purpose of the cooperation procedure is to reach a joint decision binding on the supervisory authorities and to ensure the uniform application of the GDPR across Member States. A register of decisions taken in the cross border cooperation is available on the EDPB website.

During the year, the Office of the Data Protection Ombudsman was identified as the lead supervisory authority in 22 cases and as a supervisory authority concerned in 484 cases, including cases which ended in an amicable settlement. The Office referred 66 cases to the cooperation procedure. The Office of the Data Protection Ombudsman also influenced the content of draft decisions in connection with the processing of several cases.

In spring 2025, the European data protection authorities found that TikTok has transferred the personal data of its European users to China in violation of EU data protection regulations. The Irish data protection authority imposed an administrative fine of EUR 530 million on TikTok and ordered it to bring the data transfers into compliance. The investigation conducted by Ireland showed that the company's employees in China had remote access to the data of users. The company was unable to demonstrate that a level of protection equivalent to EU requirements would be ensured for the data. Nor had it informed its users of the data transfers with sufficient transparency. In July, the data protection authorities launched a new investigation into the storage of European TikTok users' data on servers in China. The Irish supervisory authority is leading the investigation.

Decisions issued by the Office of the Data Protection Ombudsman in cross-border cooperation concerned the password policy of the online service of a gym chain, informing people about the processing of personal data, and the erasure of personal data from a social media service.

International data transfers

When personal data is transferred outside the EEA, the level of protection does not necessarily correspond to that required by the EU. Therefore, the GDPR defines criteria for transferring personal data in a secure manner. The Act on Data Protection in Criminal Cases also contains its own provisions on international data transfers. Before transferring personal data, the organisation must ensure on a case-by-case basis whether adequate protection is guaranteed for the personal data to be transferred.

In spring 2025, the Office of the Data Protection Ombudsman began an investigation into the transfer of data from the University of Helsinki to a Chinese gene technology company. The university was asked to provide information on how it has implemented the sending of data related to human research samples to China. The Data Protection Ombudsman will assess whether the university has protected personal data during the transfers as required by data protection legislation. Processing of the case will continue in 2026.

In 2025, the first BCRs for Nokia (*Binding Corporate Rules*) were confirmed in Finland. Under the BCRs, companies belonging to the same group can transfer personal data between themselves outside the EU and EEA.

Personal data can be transferred safely from European countries to outside the EEA under adequacy decisions issued by the European Commission. During the year, the EDPB issued opinions to the Commission on the continuation of the adequacy decisions on data protection in Britain and on the draft adequacy decision for Brazil. The Commission assessed the level of data protection in Britain in light of its reformed data protection legislation and adopted adequacy decisions in December 2025. In July, the Commission granted the first adequacy decision to an international organisation, the European Patent Organisation.

In September, the General Court upheld the EU–US data privacy framework with its Decision T-553/23 (Latombe v EC). The data privacy framework has been in place since July 2023, allowing companies located in the EEA to transfer personal data to US organisations that are certified and have committed to comply with the agreed safeguards. The decision has been appealed in the Court of Justice of the European Union.

In June, the EDPB published the final version of its guideline on Article 48 of the GDPR. The guideline clarifies how organisations can legally respond to requests from third country authorities to transfer or disclose personal data.

Enforcement, guidance and cooperation

Sanctions board: Administrative fines for violations of data protection legislation

The sanctions board of the Office of the Data Protection Ombudsman is tasked with processing matters concerning the imposition of administrative fines and bans on the processing of personal data. 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 2020–2025, the Sanctions Board has imposed a total of 27 administrative fines for violations of the GDPR.

In 2025, administrative fines were imposed on three organisations to a total amount of EUR 3,765,000. Administrative fines were imposed for the first time for neglecting the secure processing of personal data under the General Data Protection Regulation.

Administrative fines are one of the corrective powers of data protection authorities. 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.

Under current legislation, an administrative fine cannot be imposed on public organisations, such as the state and state-owned businesses, municipalities and parishes. A legislative drafting project of the Ministry of Justice has assessed the system of sanctions applied to violations of data protection legislation and the extension of administrative fines to public bodies. The draft Government proposal was circulated for comments in autumn 2025. In her statements, the Data Protection Ombudsman has stressed the necessity of reform, in particular to ensure the consistency, dissuasiveness and effectiveness of the sanctions system.

Administrative fines imposed in 2025

- An administrative fine of EUR 1.1 million was imposed on Yliopiston Apteekki for data protection shortcomings in the use of tracking technologies on its online pharmacy website. Information on online pharmacy use had been conveyed to tracking technology companies, such as Google and Meta, through online analytics services and other tracking technologies. The sanctions board found that the pharmacy had not adequately ensured the security of personal data generated in the use of online pharmacy services. The decision is not final at the time of publication of the annual report.

- An administrative fine of EUR 1.8 million was imposed on S-Pankki for information security shortcomings in authentication in the mobile service of its online bank. Due to a software error, it was possible to log into the online bank and online services using strong authentication with the credentials of another customer for more than three months in 2022. The sanctions board found that there had been shortcomings in how the bank had ensured the security of personal data and investigated the vulnerability. The administrative fine issued by the Financial Supervisory Authority on S-Pankki for different violations in the same sequence of events was taken into account in the amount of the administrative fine. The decision is not final at the time of publication of the annual report.

- An administrative fine of EUR 865,000 was imposed on Aktia Pankki for neglecting information security in its strong electronic authentication service. Due to a short-term technical disruption, some people logged into various e-services with Aktia's online banking codes had been able to access the data of other customers. The sanctions board found that there had been shortcomings in the planning, implementation and testing of a technical change to the service by the bank. The decision is not final at the time of publication of the annual report.

Decisions, statements and stakeholder work in different sectors

Social welfare and health care

Social welfare and health care is the largest sector for the Office of the Data Protection Ombudsman in terms of the number of cases instituted. In 2025, approximately 4,000 cases, or one quarter of all cases instituted, concerned social welfare and health care. The sector includes both private and public operators.

The high number of cases is explained, among other things, by the large number of data subjects and operators, large individual operators and the nature of the sector, as its core activities involve the processing of personal data. The processing of personal data in the social welfare and health care sector is also strictly regulated.

Most cases in the sector are notifications of personal data breaches. The majority of other cases consists of requests for accessing, rectification and erasure of client and patient data as well as complaints. The Office of the Data Protection Ombudsman also receives plenty of inquiries and requests for advice about the processing of personal data in the sector from both organisations and private individuals.

Requests concerning the exercise of data protection rights are processed with an efficient screening procedure at the Office. If necessary, the Data Protection Ombudsman can order the organisation to carry out the request. The correct handling of requests is also monitored. In 2025, the Office of the Data Protection Ombudsman clarified its decision-making practice in situations in which the controller is cautioned for the incorrect processing of a data protection request.

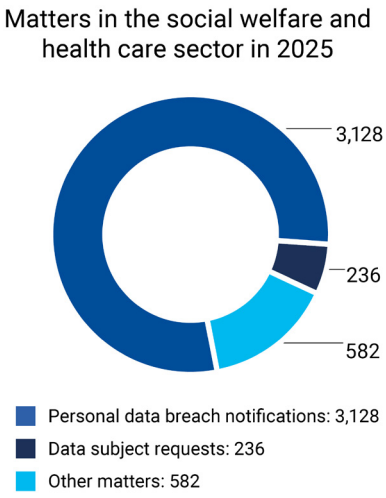
In social welfare and health care, it has been possible for individuals to obtain the access control log data for the processing of their personal data for several years now by virtue of special regulations. The interpretation made by the Court of Justice of the European Union has made access to information on the processing times and purposes of log data by virtue of the right of access under the GDPR more specific. Social welfare and health care operators must also take into account the obligations of data protection regulation when implementing the client's or patient's right of access to their personal data. The guidance published on the website of the Office regarding the right of access to log data was supplemented in summer 2025.

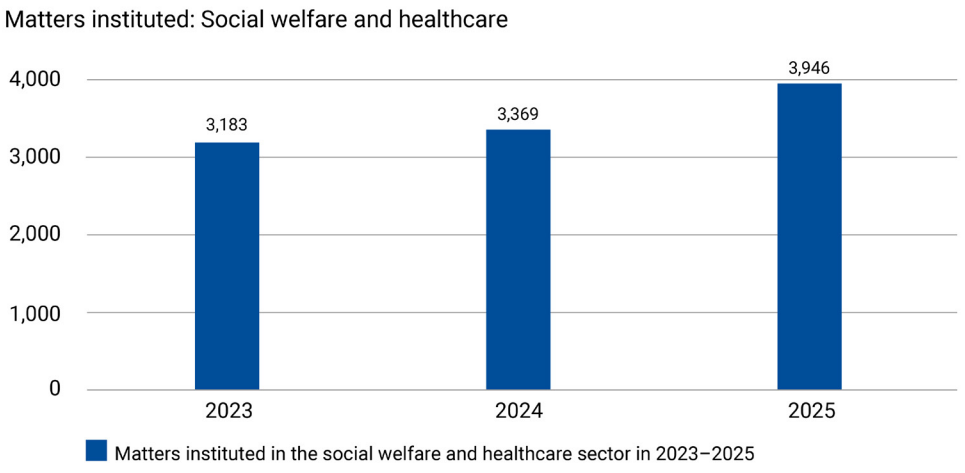
New legislation on social security in particular was introduced during the year. In October, the Data Protection Ombudsman commented on proposed amendments to the Social Welfare Act, the Act on Services for Older Persons and the Act on Client Charges in Healthcare and Social Welfare. The amendments seek to promote the use of technology in social welfare services. In addition, the Data Protection Ombudsman issued a statement on an amendment to the Act on the Secondary Use of Social and Health Data, i.e. the Secondary Use Act. The Ombudsman drew attention to the requirements concerning the security of the processing of personal data and the anonymisation of personal data, among other things.

The European Health Data Space (EHDS) Regulation entered into force on 26 March 2025, and its general application will begin in March 2027. The Regulation entails changes to the rights of patients, and the changes in national regulation will also apply to social welfare clients. In practice, Finland intends to implement the rights through the Kanta services. The Data Protection Ombudsman will continue to monitor the fulfilment of the rights going forward.

The duties of the Data Protection Ombudsman also include the processing of prior consultation requests. Before starting the processing of personal data, the controller must consult the data protection authority if the processing of personal data would involve a high risk that it has not been able to lower. During the year, the Data Protection Ombudsman processed, for example, a prior consultation request by the Social Insurance Institution concerning its Eepos development programme.

As part of its stakeholder cooperation, the Office of the Data Protection Ombudsman met key stakeholders and participated in the annual data protection seminar aimed at those working with data protection in social welfare and health care.





Financial sector

Significant precedents concerning the processing of the health data of insured persons and insurance applicants in the insurance sector were issued by the Supreme Administrative Court during the year.

In March, the Supreme Administrative Court issued its decision on the sanctions board's decision concerning the Motor Insurers' Centre (KHO:2025:23). The Supreme Administrative Court did not see any grounds for amending the Administrative Court decision by which the decision of the Office of the Data Protection Ombudsman had been revoked in 2023 and held that the Motor Insurers' Centre's method of collecting patient data to resolve claims had been lawful. The Supreme Administrative Court stressed that the insurance company's requests for information to health care operators must be justified, specific and clear. The requirement of necessity must be complied with when requesting and disclosing information. The Data Protection Ombudsman emphasises that the provision of information also requires vigilance from health care, as operators must ensure that the requested information is necessary.

In December, the Supreme Administrative Court ruled in its precedent KHO:2025:86 that an insurance company may process health data directly under the Data Protection Act when a person is applying for voluntary insurance. The Supreme Administrative Court overturned the decisions of the Data Protection Ombudsman and the Administrative Court and held that insurance companies are entitled to process the health data of an insurance applicant directly by virtue of section 6 of the Data Protection Act.

In June, the Supreme Administrative Court issued an important precedent on the right of access to user log data (KHO:2025:51). The Supreme Administrative Court found that the customer had the right to be informed of the purposes and dates of the processing of their personal data, but not of the identity of the employees who processed the data. The ruling was made on the basis of a decision of the Court of Justice in the "Bank S" case. The Supreme Administrative Court referred the matter back to the Office of the Data Protection Ombudsman, and in August the Ombudsman ordered the bank to provide the customer with the log data in accordance with the Court's ruling.

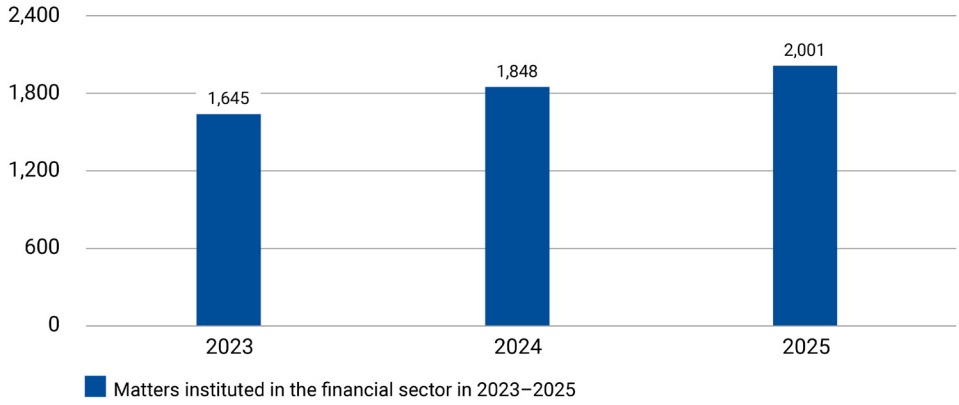
During the year, the Data Protection Ombudsman issued statements on a number of legislative proposals affecting the financial sector. For example, statements were issued on the amendments to the Act on the Incomes Information System and sections 22 and 25 of the Act on the Positive Credit Register, the Act on the Positive Credit Register and section 13 of the Act on the Residential and Commercial Property Information System, and on the repealing of section 22, subsection 2, paragraph 12 of the Act on the Positive Credit Register.

In October, the Ombudsman issued a statement on amendments to legislation under the administrative branch of the Ministry of Justice related to the overall reform of data protection legislation, which also includes changes to the conditions on which insurance companies can process the health data of individuals. In her statements, the Data Protection Ombudsman has emphasised that the processing of data must be predictable and transparent to insurance applicants, and that necessity should be a prerequisite for the processing of data.

A statement was also issued on the draft government proposal for an Act on Preventing Money Laundering and Terrorist Financing and certain related acts. The legislative amendments will implement the new EU anti-money laundering and counter-terrorist financing legislation nationally.

In the spring, the Data Protection Ombudsman published a statement on the assessment of creditworthiness based on the positive credit register in response to the shortcomings raised by Suomen Yrittäjät. The creditor is responsible for ensuring that appropriate and sufficient information is used to assess a person's creditworthiness. The Data Protection Ombudsman has already emphasised in connection with the drafting of legislation related to the positive credit register that the accuracy of data should not be compromised on when making decisions that have a significant impact on people.

Matters instituted: Financial sector



Private sector

In particular, the decisions concerning private sector operators concerned the lawful processing of personal data, informing the data subject about the processing of personal data and the exercise of data protection rights.

In her decision on direct marketing, the Deputy Data Protection Ombudsman commented on how the processing of personal data must be disclosed in telemarketing if the person's contact details have been obtained from another party than the person themselves. The key information on the processing of personal data, including information on the origin of the personal data, must be provided in a direct marketing call. A company selling natural products had not informed people as required by law during its calls and there were also shortcomings in its practices concerning data protection requests. The Office also supplemented the instructions published on its website regarding the information to be provided in connection with telemarketing.

In May, the Deputy Data Protection Ombudsman issued a decision concerning the legal basis for the processing of personal data. A debt collection agency had unlawfully processed the personal data of a resident who had rented a parking space when collecting undue parking fines. As parking control and the conditions of parking had not been agreed on in the lease agreement for the parking space, the parking fines were unfounded and the debt collection agency had no right to process the resident's personal data when collecting them. The decision is not final.

In January, the Office of the Data Protection Ombudsman began investigating a data breach that had been detected in Valio's information network in December 2024 as a personal data breach. The attacker had obtained data of current and former Valio employees and the personnel of Valio's subsidiaries and milk purchase cooperatives in Finland. The Office requested clarifications from the companies affected by the data breach. Based on these clarifications, the Office will assess whether the companies have complied with their obligations arising from data protection legislation. The investigation will continue in 2026.

Significant decisions concerning the private sector were made by the administrative courts in 2025. In February, the Supreme Administrative Court issued precedent KHO:2025:15 on the publication of tax information on tax information portals operated by the media and gave the decision of the Data Protection Ombudsman legal force. The Supreme Administrative Court held that the media had no obligation to erase the appellant's data from tax information portals, as the data was being processed for journalistic purposes. Certain provisions of the GDPR do not apply to journalistic activities.

The sanction board's decision on the administrative fine imposed on Suomen Yritysrekisteri was made final by a decision of the Administrative Court of Eastern Finland in March.

Some growth in the number of cases was observed during the year, especially in cases related to technology and digital services. The communications received showed, among other things, the "consent or pay" policy introduced by a tabloid for targeted online advertising and the update of Posti's terms of use. Communications concerning international digital giants stood out in matters related to social media and games, most of which will be handled in cross-border cooperation between EU countries.

Judicial, security and other public administration

In the public sector, guidance and enforcement activities are focused on several different fields. More specific and supplementary legislation is applied to the various branches of the public sector in addition to the General Data Protection Regulation and the Act on Data Protection in Criminal Cases.

Most of the cases concerning central government and municipalities were related to personal data breaches and the exercise of individuals' data protection rights, such as access to or erasure of personal data. With regard to registers of multiple security authorities, an individual may exercise their right of access to their personal data through the Data Protection Ombudsman.

A decision package on the use of cloud services in central government was issued in October. The procedures of the Government ICT Centre Valtori, the Digital and Population Data Services Agency and the Tax Administration in February–April 2022 were evaluated. The investigation found that sufficient protection had not been ensured for personal data when it was transferred to the United States through the cloud service provided by Valtori. The EU and the US did not have a data transfer arrangement in place during this period that would have allowed for the secure transfer of data. For this reason, the organisations were obliged to ensure by means of various additional safeguards that the required level of data protection was maintained in data transfers. The investigation was part of a more extensive EU report, in which data protection authorities examined the use of cloud services by approximately one hundred public sector organisations in the Member States.

During the year, the Data Protection Ombudsman drew attention to the authorities' right of access to information in several statements concerning legislative amendments. In February, the Ombudsman commented on the draft amendment to the Act on the Processing of Personal Data by the Police, the Act on the Processing of Personal Data by the Immigration Administration, section 131 of the Aliens Act and chapter 2, section 1 of the Police Act. The amendments would give the police the right to use fingerprints and other biometric identifiers in criminal investigations. The Data Protection Ombudsman emphasised that, in further preparation, attention should be paid to assessing proportionality with regard to the objectives. In addition, the use of data for a purpose other than the original one should be justified in more detail, and the risks to people should be carefully assessed.

In August, the Data Protection Ombudsman issued her statement on a proposal to amend the legislation concerning the exchange of information by the police. The proposal would extend the right of the police to disclose information and clarify police access to information from, for example, the social welfare and health care sector and private operators, such as communications intermediaries or information society service providers. Particular attention was paid to the assessment of risks and data protection impacts as well as the precise scope of regulation. In the field of security administration, the Ombudsman also issued statements on such matters as the amendment of the Coercive Measures Act, automatic retrieval and exchange of information in police cooperation and legislative amendments concerning the exchange of information between different authorities in crime prevention.

The Government proposed amendments to the regulation of the Tax Administration's comparative information audits to combat tax evasion (section 21 of the Act on Taxation Procedure). According to the proposal, the Tax Administration's right of access to information would be extended so that it would receive data on people's transactions from banks for tax supervision purposes. In her statements and opinions, the Data Protection Ombudsman emphasised that the proposal would significantly curtail the fundamental right to privacy and would give the Tax Administration the right to also process large amounts of personal data that are unnecessary for tax supervision. The Ombudsman reminded the legislators that the powers of the authorities should be precisely defined, and that tax evasion should be prevented with targeted and proportionate measures. The bill has been amended on the basis of the observations made in the statement of the Constitutional Law Committee.

During the year, statements were also issued on an amendment to the Archives Act and the Act on Information Management in Public Administration. The Data Protection Ombudsman paid particular attention to the definition of roles in personal data processing and the storage periods of data, the basis for processing in different situations and the fulfilment of people's data protection rights. Clarifications were called for, in particular with regard to the archiving of sensitive personal data such as genetic data.

The EU NIS2 Directive on critical sectors of society was implemented nationally by the Cybersecurity Act, which entered into force in April 2025. The supervisory authorities referred to in the Cyber Security Act are obliged to notify the Data Protection Ombudsman of personal data breaches coming to their attention. A notification submitted by the supervising authority does not supersede the controller's duty to notify.

During its Presidency of the Council of the EU, Denmark submitted a new compromise proposal on the CSAM Regulation on combating online child sexual abuse. At the beginning of November, the EU Member States reached an agreement on the Council's position on the content of the Regulation. The new proposal abandoned a large-scale and untargeted obligation to scan message content.

As part of its stakeholder cooperation, the Office of the Data Protection Ombudsman participated in the work of the VAHTI network. The network is a cooperation body for digital security in public administration and an expert network that develops cyber and digital security broadly in Finland. In addition, the Office participated in the development of municipal data protection work in a project led by the Association of Finnish Cities and Municipalities. A guideline was drawn up in the project to help establish common concepts and the organisation of data controllers in municipalities.

Statements in criminal matters

At the request of the prosecutor or the pre-trial investigation authority, the Data Protection Ombudsman has a duty to issue statements on four offences provided for in chapter 38 of the Criminal Code: data protection offences, secrecy offences, unlawful access to an information system and violations of the secrecy of communications. The purpose of the statements is to ensure sufficient data protection expertise in the consideration of charges.

The number of requests for statements in criminal matters increased from the previous year. For example, an increase has been observed in the number of statements requested on violations of the secrecy of communications. Most of the statements concerned data protection offences, such as "snooping". In cases of snooping, an employee or office holder has viewed personal data without a justified reason.

During the year, statements were issued on a number of large-scale criminal cases. In these cases, an individual had viewed the data of several persons or several persons had viewed the data of a single individual.

Education

The Office of the Data Protection Ombudsman issued several statements to the Ministry of Education and Culture and Parliament. The Ministry was issued with a statement on the amendment of the legislation on language examinations. The degree process is being gradually digitalised, with the aim to ultimately make degrees fully electronic.

The Data Protection Ombudsman also issued a statement on the proposal for an Act on the National Data Repository, which is part of the digital Competency Path service. The purpose of the data repository is to support individuals in applying for education and training and finding employment, the maintenance of competencies, the utilisation of education and career data, as well as anticipation and maintaining situational awareness. The service can make use of automated processing to suggest training and job opportunities to an individual. Personal data can also be used for the development of AI functionalities in the service. The statement emphasised that the deployment and development of AI systems must also comply with data protection legislation.

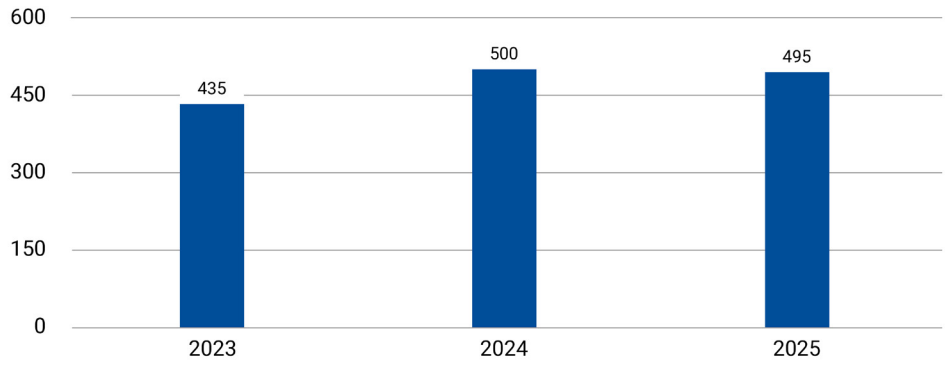
In a decision issued in March, the Deputy Data Protection Ombudsman commented on the processing of the fingerprint data of pupils. A city distributed public swimming pool access bracelets to pupils in basic education, with fingerprint data stored in the bracelets for access control. The Deputy Data Protection Ombudsman found that the city had not defined a basis for the processing of personal data before the implementation of the method, as it had considered that it did not involve the processing of personal data. A data protection impact assessment should have been conducted of the introduction of dactyloscopic bracelets, as it is a new technology that is likely to pose a high risk to the rights and freedoms of individuals.

The Deputy Data Protection Ombudsman cautioned a student union because the attachments of meeting agendas containing personal data had been stored publicly online for several years in a folder linked to the union's website. This was revealed by a data breach notification made by the student union. The Deputy Data Protection Ombudsman found that the student union had not supervised its processing of personal data appropriately, prepared sufficient instructions on the processing of attachments or ensured the data protection competence of persons working under it.

The Supreme Administrative Court issued its decision on the decision of the Office of the Data Protection Ombudsman, which had assessed the legality of the use of an electronic teaching platform in basic education in the City of Espoo. The Supreme Administrative Court overturned the decisions of the Helsinki Administrative Court and the Data Protection Ombudsman and returned the matter to the Office for reassessment. The reassessment was begun during the year.

At the end of November, the Office participated in the education sector's annual seminar.

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 2023–2025. Statistics on youth work have been compiled since 2024.

Inspection activities

Inspections are one of the ways in which the Office of the Data Protection Ombudsman detects shortcomings in data protection and guides organisations into compliance with data protection legislation. They are also an effective means of enforcing compliance with the authority's orders. Inspections are carried out in accordance with an annual plan and where necessary. The inspection activities of the Office are guided by risks related to the processing of personal data, the identified need to supervise a certain controller or sector, and statutory inspection obligations. An inspection may target individual or multiple operators or entire sectors.

For the first time, the Office of the Data Protection Ombudsman prepared its annual inspection plan on a multiannual basis. The plan included a plan for 2026–2027, to be supplemented later. Eight inspections were completed in 2025. Two inspections begun or planned during the year are expected to be completed in 2026.

As in previous years, the inspections focused on the procedures of the security authorities, as the individuals themselves only have limited access to information on the processing of personal data carried out by them. In cooperation with the Intelligence Ombudsman, the Data Protection Ombudsman inspected the processing of personal data related to intelligence in the Defence Forces. Inspections were also targeted at other internal security authorities and, for example, biobanks. The inspections carried out during the year also included periodic statutory inspections to be conducted by the Office of the Data Protection Ombudsman. These included inspections of the SIS, VIS and Eurodac systems. In addition, an inspection of rescue services operating in wellbeing services counties was launched.

Findings of the inspections concerned the clarity of roles and responsibilities in processing personal data, keeping competencies and access rights up to date, data life cycle management and impact assessments.

The organisations were issued with guidance and recommendations based on the findings of the inspections. In particular, these findings concerned the clarity of roles and responsibilities in processing personal data, keeping competencies and access rights up to date, data life cycle management and impact assessments.

The first inspection focused on parking control activities was carried out in the private sector. It found that ParkkiPate Oy had complied with the previous orders issued by the Data Protection Ombudsman on the erasure of personal data related to parking fines. Based on the findings, the Ombudsman recommended that the company explain the storage periods of personal data and the information disclosed to debt collection agencies more clearly in its privacy statement.

During the year, 32 data protection authorities in EU and EEA countries investigated how organisations implement the right of individuals to have their personal data erased. The investigation was a joint measure coordinated by the EDPB to implement EU-level strategic objectives. The right to erasure is one of the most commonly exercised data protection rights, and the authorities receive a large number of complaints concerning it.

In Finland, the implementation of the right to erasure was investigated by means of an anonymous and voluntary survey directed at all higher education institutions, debt collection agencies and insurance and employment pension insurance companies. The survey was sent to 61 organisations and 37 responses were received. In particular, the choice of sectors reflected the frequency of erasure requests and the amendment to the Credit Information Act that entered into force in 2022 and shortened the statutory storage periods for payment default entries. The aim of the survey was to obtain general information on the challenges faced by organisations.

In February 2026, the EDPB published a report on the investigation, which issues recommendations for answering seven challenges. Challenges were identified in the procedures for processing requests, the definition of personal data storage periods, the erasure of data in connection with making backups, effective anonymisation, and informing people about the right to erasure. In addition, difficulties were identified in balancing the right of erasure with other rights and in the assessment of the prerequisites for and exceptions to exercising the right. The right to erasure does not exist in all situations. Based on the report, guidance materials were prepared for the website of the Office of the Data Protection Ombudsman.

Guidance and communications

Proactive guidance is a key part of a data protection authority's work. The guidance is of a general nature and no detailed or binding opinions are given.

During the year, the Office of the Data Protection Ombudsman responded to more than 1,300 written requests for guidance and advice. The Office's telephone service provides general guidance on data protection and the processing of personal data. There are dedicated service numbers for private individuals and organisations. The telephone service answered a total of 2,579 calls, which represents a slight decrease from the previous year. The majority of calls to the guidance service are made by private individuals. Telephone guidance is not included in the statistics on the total number of cases instituted.

Questions commonly answered by the general guidance service concerned people's data protection rights in various sectors, personal identity codes, social welfare and health care log data, and personal data processing roles in organisations. Questions about data protection in working life and camera surveillance were also common.

As in previous years, personal data breaches were reflected in enquiries made by both individuals and organisations. The organisations' enquiries typically concerned the definition of a data breach and what to do in case of a suspected data breach. Private individuals contact the Office of the Data Protection Ombudsman more often after major cases that receive publicity, such as the data breach against Valio's information network, the effects of which were felt in January 2025. Private individuals turn to the Office, for example, if the controller's contact channels are unclear or the information received from the organisation is considered insufficient.

The need for information is also addressed through guidance provided on the website of the Office. During the year, guidelines were drawn up and updated on topical themes, such as employee substance abuse testing, data protection in housing, right of access to personal data, right of access to log data and the processing of personal data in connection with direct marketing.

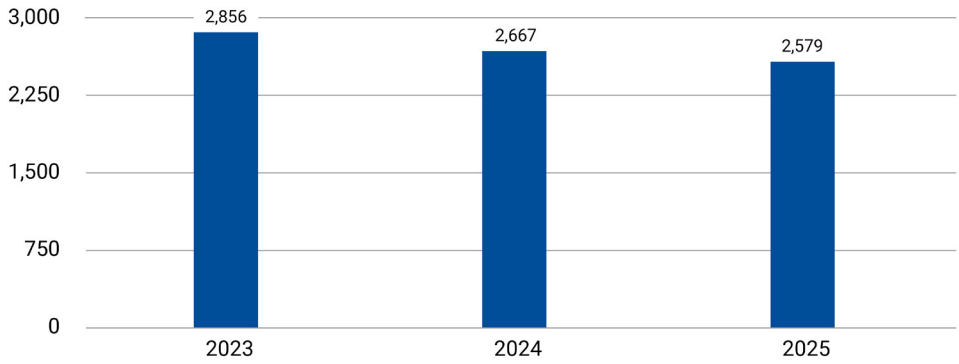
In the spring, the Office of the Data Protection Ombudsman published instructions on taking data protection into account in AI systems. If an AI system involves the processing of personal data, its development and use must comply with data protection legislation. AI systems are also regulated by the EU AI Act. An organisation developing or using an AI system must assess the processing of personal data, the associated risks and the requirements arising from legislation on a case-by-case basis.

In the spring, parties and others involved in electoral campaigns were reminded of taking data protection into account in the campaigning for the county and municipal elections. The transparency of personal data processing and fundamental rights must also be safeguarded when political advertising is targeted on the basis of personal data on social media. The obligations concerning the transparency of advertising must also be complied with.

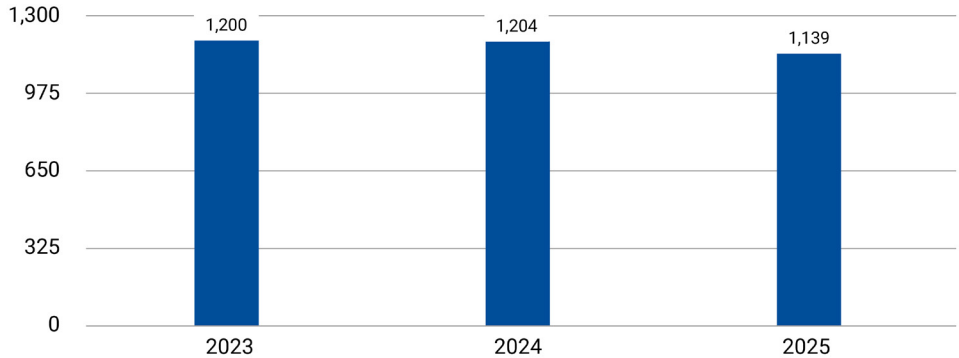
The Data Protection Day event was organised for the sixth time on International Data Protection Day in January in cooperation with Alma Insights.

Each year, the event brings approximately 500 data protection professionals to Helsinki to listen to talks on topical issues.

Answered phone calls in the telephone guidance service



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

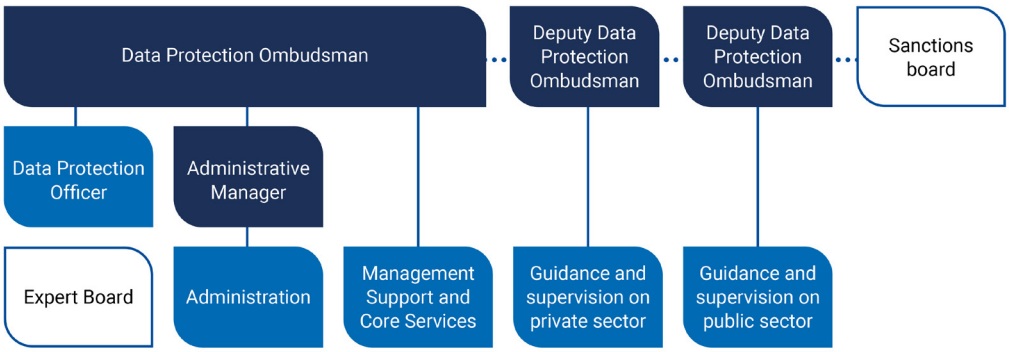


Organisation, personnel and finances

The Agency for Special Authorities in Judicial Administration started operations on 1 January 2025. The Office of the Data Protection Ombudsman is administratively a part of this agency consisting of 11 independent authorities and a unit providing administrative services for them.

The number of personnel employed by the Office of the Data Protection Ombudsman increased during the year under review. At the end of the year, 64 people worked in the Office, contributing 61.4 person-years in 2025.

Organisation structure of the Data Protection Ombudsman



The Office's organisational structure consists of four units: the Private Sector Guidance and Supervision Unit (YKI), the Public Sector Guidance and Supervision Unit (JUKI), the Administration Unit (HALL) and the Management Support and Core Services Unit (EKY). The Data Protection Ombudsman leads the Management Support and Core Services Unit, the Deputy Data Protection Ombudsman the YKI and JUKI units and the Administrative Manager the Administration Unit.

In 2025, a team responsible for international affairs and EU cooperation and a team of specialised IT experts were set up in the Management Support and Core Services Unit under their own team leaders. The team leaders of the YKI, JUKI and EKY units act as the administrative supervisors of their unit members and support them in their work. The EKY unit also includes communications personnel, a special adviser and the Data Protection Officer. The Office's administration,

information management, registry services and management support have been centralised in the Administration Unit.

In 2025, the Office of the Data Protection Ombudsman launched a reform of its organisational structure. Going forward, operations will be organised into areas of responsibility based on sectors and fields of activity. The reform will also create structures for the performance of the data protection authority's new enforcement duties, especially those arising from EU regulation, such as the enforcement of the AI Act. The aim is to enhance supervisory work, improve the division of labour and allocate management resources appropriately.

The resources of the Data Protection Ombudsman will be boosted by a EUR 2.35 million transfer of appropriations from 2026. The resource increase will enable the Office to recruit several new full-time employees from 2026. They will include senior inspectors serving as team leaders of the new areas of responsibility. The first new positions were opened for application in November 2025.

Well-being at work was one of the focus areas of the Office's strategy for 2022–2025. During the year under review, emphasis was placed on the resources of the work community, which enable the high-quality performance of our duties. These resources include adequate financial and human resources, the well-being of personnel and sufficient preparation for new duties. A development project has been under way at the Office since 2024, with two sub-projects focusing on work processes and the organisation of work as well as on the work community and work culture.

Finances of the Office of the Data Protection Ombudsman	Realisation 2023	Realisation 2024	Target 2025	Realisation 2025
Use of the operating expenses appropriation, €1,000	4,324	4,991	5,491	5,582
Total costs, €1,000	4,730	5,853	-	5,582

Human resources*	2023	2024	2025
Number of personnel at the end of the year	54	60	64
Person years	52.7	61.4	61.4
Average age	42.1	40.9	40.6
Education index	6.4	6.5	6.5

* Figures for 2024 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.

Annexes

Matters instituted and processed in 2023–2025

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 2023–2025. 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.

	2023		2024		2025	
	Instituted	Processed	Instituted	Processed	Instituted	Processed
Tasks in accordance with the GDPR and the Data Protection Law Enforcement Directive						
Prior consultation (high risk)	23	25	11	8	7	8
Statements	287	301	160	145	152	155
Statements in criminal cases*			98	110	89	120
Codes of Conduct	0	2	0	1	0	1
Transfers of personal data	3	18	7	57	30	31
EU and international cooperation	1,362	1,297	1,39	1,131	1,8	1,408
Rights of the data subject	838	994	797	819	1,144	1,017
Supervision	1,268	1,197	1,276	1,173	1,832	1,767
Personal data breaches	6,894	6,487	7,152	7,467	7,355	7,622
Guidance and advice	1,318	1,592	1,209	1,247	1,316	1,309
Data Protection Officers	267	260	473	459	913	822
Board of Experts	2	2	1	1	0	0
Other	0	0	0	0	0	1
General, financial and human resource issues	917	884	710	673	770	772
Total	13,179	13,059	13,284	13,291	15,408	15,033

* Separate statistics since 2024

Statements issued by the Office of the Data Protection Ombudsman in 2025

Statements on legislative projects

- Statement on the draft government proposal to Parliament for legislation on a digital service package for continuous learning (9 January 2025)
- Statement on a temporary amendment to the Act on Transport Services (29 January 2025)
- Statement on an assessment memorandum on sanctions against authorities for violations of data protection legislation (31 January 2025)
- Statement on a draft government proposal to Parliament for acts amending the Act on the Processing of Personal Data by the Police, the Act on the Processing of Personal Data by the Immigration Administration, section 131 of the Aliens Act and chapter 2, section 1 of the Police Act (21 February 2025)
- Statement on a draft government proposal to Parliament for acts amending the Act on the Grey Economy Investigation Unit and certain related acts (24 February 2024)
- Statement on a draft government proposal to Parliament for the Archives Act and an act amending the Act on Information Management in Public Administration (13 March 2025)
- Statement on a draft government proposal to Parliament for an Act on the Housing Savings System and related acts (13 March 2025)
- Statement on a draft government proposal to Parliament for an Act amending chapter 8, section 29 of the Coercive Measures Act (19 March 2025)
- Statement on a draft government proposal to Parliament for legislation on the development of the jobseeker's service process and employment services (27 March 2025)
- Statement on a draft government proposal for acts amending the Act on the Natural Resources Institute Finland and the Act on Food and Natural Resources Statistics (14 April 2025)
- Statement on a draft government proposal for amending the Act on the Secondary Use of Social and Health Data and certain other acts (24 April 2025)
- Statement on a draft government proposal and Government Decree on amending the legislation on asbestos work and professional qualifications in occupational safety and health (24 April 2025)
- Statement on a draft government proposal for regulation supplementing the European Health Data Space (EHDS) Regulation (8 May 2025)
- Statement on a draft government proposal for the Act on Digital Information Services in the Transport System and related Acts (9 May 2025)

- Statement on a draft government proposal to Parliament for acts amending the Act on the Social Insurance Institution of Finland and certain other acts (9 May 2025)
- Statement on a draft Government proposal to Parliament for legislation supplementing the EU Regulation on the transparency and targeting of political advertising (9 May 2025)
- Statement on a draft government proposal amending the Act on the Supervision of Certain AI Systems (28 May 2025)
- Statement on a draft government proposal for amending the Act on Transport Services and certain related acts (taxis) (31 May 2025)
- Statement on a draft government proposal for the Act on the Implementation of the Truth and Reconciliation Process for Deaf People and Sign Language Users (12 June 2025)
- Statement on a draft government proposal to Parliament amending the Act on Social Assistance, section 64 of the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare and section 10 of the Act on Rehabilitative Work Activities (17 June 2025)
- Statement on a draft government proposal for an act amending the Health Care Act and certain related acts (18 June 2025)
- Statement on a draft government proposal to Parliament for an act amending the Act on Child Maintenance Allowance, Child Maintenance Act and the Act on the Incomes Information System (18 June 2025)
- Statement on a draft government proposal for amending the Health Care Act and Client Data Act (23 June 2025)
- Statement on a government proposal to Parliament for the Act on a Limited Liability Company Called Finnfund Oy and certain related acts (30 June 2025)
- Statement on a draft government proposal to Parliament for a new Land Use Act (1 July 2025)
- Statement on a draft government proposal to Parliament on amending the legislation on language examinations (8 July 2025)
- Statement on a government proposal to Parliament for legislation on the implementation of the EU Listing Act (17 July 2025)
- Opinion on the draft Decree of the Ministry of Agriculture and Forestry on the Patient Register of a Veterinarian (30 July 2025)
- Statement on a draft government proposal for amending the Act on Electronic Prescriptions and certain related acts (13 August 2025)

- Statement on a draft government proposal to Parliament for legislation on the reform of the pharmacy economy and the implementation of pharmaceutical savings and the related proposed decree amendments (14 August 2025)

- Statement on a draft government proposal for acts amending the Police Act, Act on the Processing of Personal Data by the Police, Act on the Processing of Personal Data by the Border Guard, Act on the Administration of the Border Guard, Act on the Prevention of Crime by Customs, Act on the Processing of Personal Data by Customs and Act on the Processing of Personal Data by the Immigration Administration (14 August 2025)

- Statement on a draft government proposal to Parliament for an act amending section 21 of the Act on Taxation Procedure (29 August 2025)

- Statement on a draft Government proposal to Parliament for the Act on Preventing Money Laundering and Terrorist Financing and certain related acts (5 September 2025)

- Request for a statement on a draft government proposal to Parliament for legislation supplementing the EU Regulation on electronic identification, trust services and the European digital identity (12 September 2025)

- Statement on a draft government proposal to Parliament for the approval and enforcement of the Family and Spouse Agreement between Finland and the United States (24 September 2025)

- Statement on a draft government proposal on amendments to legislation under the administrative branch of the Ministry of Justice related to the overall reform of data protection legislation (8 October 2025)

- Statement on a draft government proposal to Parliament for acts amending the Act on the Processing of Personal Data by the Prison and Probation Service of Finland, the Enforcement Code and certain other acts (13 October 2025)

- Statement on a draft government proposal to Parliament on the amendment of the Data Protection Act and Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (13 November 2025)

- Statement on a draft government proposal for amending the Act on Automatic Retrieval and Exchange of Information in Police Cooperation and the Act on the Processing of Personal Data by the Police (30 December 2025)

Written expert opinions to parliamentary committees

- Expert opinion to the Constitutional Law Committee on a government proposal to Parliament for amending the Act on Transport Services (HE 182/2024 vp)
- Expert opinion to the Employment and Equality Committee on the Act on the Registration of Occupational Safety and Health Cooperation Officers and acts amending section 47 of the Act on Occupational Safety and Health Enforcement and Cooperation on Occupational Safety and Health at Workplaces and the Chargers Act (11 February 2025)
- Expert opinion to the Transport and Communications Committee on a government proposal to Parliament for an act amending the Act on Transport Services (HE 182/2024 vp) (17 February 2025)
- Expert opinion to the Constitutional Law Committee on a government proposal to Parliament for an Act amending the Act on Preventing Money Laundering and Terrorist Financing and related Acts (HE 157/2024 vp) (21 February 2025)
- Expert opinion to the Tax Sub-Committee of the Finance Committee on a government proposal to Parliament for acts amending the Act on the Incomes Information System and sections 22 and 25 of the Act on the Positive Credit Register (HE 216/2024 vp) (25 February 2025)
- Expert opinion to the Transport and Communications Committee on a government proposal for an act amending the Vehicles Act and related acts (HE 3/2025 vp) (27 February 2025)
- Expert opinion to the Legal Affairs Committee on a government proposal to Parliament for an act amending the Act on the Enforcement of Fines and certain related acts (HE 5/2025 vp) (5 March 2025)
- Expert opinion to the Constitutional Law Committee on a government proposal to Parliament for acts amending the Act on a Candidate's Election Funding, the Act on Political Parties, the Election Act and section 10 of the Citizens' Initiative Act (HE 190/2024 vp) (12 March 2025)
- Expert opinion to the Administration Committee on a government proposal to Parliament for an act amending the Aliens Act (HE 10/2025 vp) (24 March 2025)
- Expert opinion to the Grand Committee on a government communication on the European Commission's proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (COM(2022) 209 final) (2 May 2025)
- Expert opinion to the Transport and Communications Committee on a government proposal to Parliament for a temporary amendment to the Act on Transport Services (HE 33/2025 vp) (9 May 2025)
- Expert opinion to the Constitutional Law Committee on follow-up communication UJ 2/2025 vp – U 69/2022 vp to the government communication on the European Commission's proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (COM(2022) 209 final) (12 May 2025)

- Expert opinion to the Transport and Communications Committee on a government proposal to Parliament for acts amending the Cyber Security Act and section 3 of the Act on Information Management in Public Administration (HE 27/2025 vp) (16 May 2025)

- Expert opinion to the Legal Affairs Committee on a government proposal for acts amending the Act on the Positive Credit Register and section 13 of the Act on the Residential and Commercial Property Information System and repealing section 22, subsection 2, paragraph 12 of the Act on the Positive Credit Register (HE 43/2025 vp) (19 May 2025)

- Expert opinion to the Finance Committee on a government proposal for acts amending the Act on the Positive Credit Register and section 13 of the Act on the Residential and Commercial Property Information System and repealing section 22, subsection 2, paragraph 12 of the Act on the Positive Credit Register (HE 43/2025) (19 May 2025)

- Expert opinion to the Constitutional Law Committee on a government proposal to Parliament for acts amending the Act on the Monitoring System of Bank and Payment Accounts, the Act on Taxation Procedure and section 30 of the Act on the Taxation Procedure for Self-Assessed Taxes (HE 25/2025 vp) (19 May 2025)

- Expert opinion to the Administration Committee on a government proposal to Parliament for acts amending the Act on the Monitoring System of Bank and Payment Accounts, the Act on Taxation Procedure and section 30 of the Act on the Taxation Procedure for Self-Assessed Taxes (HE 25/2025 vp) (19 May 2025)

- Expert opinion to the Economic Affairs Committee on a government proposal to Parliament for legislation supplementing the EU AI Act (HE 46/2025 vp) (23 May 2025)

- Expert statement to the Education and Culture Committee on a government proposal to Parliament for legislation supplementing the EU AI Act (HE 46/2025 vp) (23 May 2025)

- Expert opinion to the Administration Committee on government communication U 15/2025 vp to Parliament on the European Commission's proposal for the return of third-country nationals staying illegally in the Union (2025/0059(COD), return regulation proposal) (6 June 2025)

- Expert opinion to the Constitutional Law Committee on a government proposal for acts amending the Act on the Positive Credit Register and section 13 of the Act on the Residential and Commercial Property Information System and repealing section 22, subsection 2, paragraph 12 of the Act on the Positive Credit Register (HE 43/2025) (6 June 2025)

- Expert opinion to the Legal Affairs Committee on a government proposal for legislation supplementing the EU Regulation on the transparency and targeting of political advertising (HE 57/2025 vp) (12 June 2025)

- Expert opinion to the Administration Committee on a draft Government proposal to Parliament for an Act amending chapter 5a of the Police Act and certain other acts (HE 29/2025 vp) (29 August 2025)

- Statement on follow-up communication UJ 2/2025 vp – U 69/2022 vp to the government communication on the European Commission's proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (COM(2022) 209 final) (5 September 2025)

- Expert opinion on a government communication to Parliament on the Commission's proposals for amending directives and regulations of the European Parliament and of the Council to reduce the regulatory burden on small midcap companies (Omnibus IV proposals) (U 30/2025 vp) (9 September 2025)

- Expert opinion to the Constitutional Law Committee on a government proposal to Parliament for an Act amending the Act on the Secondary Use of Social and Health Data and related acts (HE 87/2025 vp) (2 October 2025)

- Expert opinion to the Employment and Equality Committee on a government proposal to Parliament for legislation on the development of the jobseeker's service process and employment services (HE 108/2025 vp) (8 October 2025)

- Expert opinion to the Social Affairs and Health Committee on the Government proposal to Parliament for an Act amending the Act on the Secondary Use of Social and Health Data and related acts (HE 87/2025 vp) (8 October 2025)

- Expert opinion to the Social Affairs and Health Committee on a government proposal to Parliament for an act amending the Act on the Social Insurance Institution of Finland, the Act on the National Audit Office of Finland and the Act on the Incomes Information System (HE 81/2025 vp) (9 October 2025)

- Expert opinion to the Education and Culture Committee on a government proposal to Parliament for the Act on the National Data Repository and related acts (HE 133/2025 vp) (13 October 2025)

- Expert opinion to the Social Affairs and Health Committee on a government proposal to Parliament for acts amending the Act on Child Maintenance Allowance, Child Maintenance Act and section 13 of the Act on the Incomes Information System (HE 115/2025 vp) (13 October 2025)

- Expert opinion to the Constitutional Law Committee on a government proposal to Parliament for acts amending the Social Welfare Act, Act on Supporting the Functional Capacity of the Older Population and on Social and Health Services for Older Persons and Act on Client Charges in Healthcare and Social Welfare (HE/113/2025 vp) (21 October 2025)

- Expert opinion to the Employment and Equality Committee on a government proposal to Parliament for the Act on the Implementation of the Truth and Reconciliation Process for Deaf People and Sign Language Users in 2026–2028 (HE 82/2025 vp) (21 October 2025)

- Expert opinion to the Transport and Communications Committee on a government proposal to Parliament for legislation supplementing the EU Data Act (HE 128/2025 vp) (14 October 2025)

- Expert opinion to the Education and Culture Committee on a draft government proposal to Parliament for the Archives Act and an act amending the Act on Information Management in Public Administration (HE 169/2025 v) (24 November 2025)

- Expert opinion to the Constitutional Law Committee on a government proposal to Parliament for an Act on the National Data Repository and related acts (HE 133/2025 vp) (30 October 2025)

- Expert opinion to the Constitutional Law Committee on a government proposal to Parliament for an act amending section 21 of the Act on Taxation Procedure (HE 141/2025 vp) (10 November 2025)

- Expert opinion to the Grand Committee on a government communication on the European Commission's proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (U 69/2022 vp) (25 November 2025)

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