



OFFICE OF  
THE DATA PROTECTION OMBUDSMAN

ANNUAL REPORT  
OF THE OFFICE OF THE DATA  
PROTECTION OMBUDSMAN 2022

ANNUAL REPORT  
OF THE OFFICE OF THE DATA  
PROTECTION OMBUDSMAN 2022



# Contents

The Office of the Data Protection Ombudsman safeguards the rights and freedoms of individuals with regard to the processing of personal data .....	4
Data Protection Ombudsman Anu Talus – Trust is crucial in the data economy.....	6
Deputy Data Protection Ombudsman Heljä-Tuulia Pihamaa: Children’s data protection, patient and client data processing and other public-sector data protection issues .....	9
Deputy Data Protection Ombudsman Annina Hautala: A diverse data protection year in security and the judicial administration .....	12
Office of the Data Protection Ombudsman’s year 2022 in figures .....	14
Focus areas of data protection activities.....	16
Sanctions Board: Administrative fines for violations of data protection legislation.....	16
Renewed strategy, closer European cooperation .....	18
Backlog clearing and new processes .....	19
Continued increase in personal data breach notifications.....	20
Processing cross-border matters .....	21
Projects to support controllers .....	23
International transfers of data and cloud services .....	24
Auditing activities.....	26
Personnel and finances – reform of the organisation launched .....	27
Focus areas for 2023 and future developments.....	29
Matters instituted and processed from 2020 to 2022.....	31

# 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 laws 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 studies and inspections, issuing statements on legislative and administrative reforms and imposing sanctions for violations of the General Data Protection Regulation (GDPR). The Data Protection Ombudsman cooperates with the

data protection authorities of other countries and represents Finland on the European Data Protection Board (EDPB).

In 2022, Anu Talus served as Data Protection Ombudsman and Heljä-Tuulia Pihamaa as Deputy Data Protection Ombudsman. Jari Râman served as the second Deputy Data Protection Ombudsman until May 2022. Master of Laws Annina Hautala took up the position of Deputy Data Protection Ombudsman in September.

## Societal objectives of the Office of the Data Protection Ombudsman

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

## Mission

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

# Data Protection Ombudsman Anu Talus – Trust is crucial in the data economy

The significance of digitisation, the data economy and information security were major themes in a seminar on the future arranged by the Ministry of Finance Ministerial Working Group on Developing the Digital Transformation, the Data Economy and Public Administration in the spring of 2023. The next trend was said to be trust. There is a name for such trust: data protection. A fundamental right upon which the European data economy is being built.

You could probably call 2022 a year of establishment. Meanwhile, the past year was also marked by reforms and development. This is also a well-established phenomenon – evolving technology and legislation to respond to the changes keep data protection in a constant state of flux. A data protection specialist is always facing something new.

The first sign of levelling off is the number of matters instituted at the Office of the Data Protection Ombudsman. For the third year in a row, some 11,000 matters were instituted. The stabilised volume also makes it easier to organise the work at the office.

Another development that illustrates the establishment of the activities involves decisions made by the sanctions board of the

Office of the Data Protection Ombudsman. During the year, the sanctions board issued five decisions imposing administrative fines ranging from EUR 8,300 to EUR 750,000. None of the decisions made by the sanctions board were appealed to the Administrative Court. This was not the case with the first decisions of the sanctions board, which were regularly appealed regardless of the amount of the administrative fine. This change may be partly due to the fact that the Administrative Court has confirmed that in terms of procedural issues, the practices of the Office of the Data Protection Ombudsman are in line with the legislative requirements. In addition, the administrative fine is no longer a new sanction, and there is an established practice for the size of the fine and an understanding of the pan-European level. Examples of cases where administrative fines were imposed included ones where there were deficiencies concerning the core business of the controller, where internal procedures were not appropriate or where cooperation with the authority had been avoided.

Other decisions worth mentioning include a decision by the Finnish Tax Administration on too extensive collection of data, a decision by the Deputy Data Protection Ombudsman which stated that the data subject's right to

inspect is not a means for an authority to obtain information, and a decision by the Deputy Data Protection Ombudsman which stated that the location data feature cannot be automatically switched on in an employee's work device.

Questions on international transfer of personal data also seem to be a well-established topic. The coordinated action of the European Data Protection Board in 2022 focused on the use of cloud-based services in the public sector. Meanwhile, several member states are dealing with "101 Dalmatians" complaints, where the core issue is the same – data transfer to third countries. A decision by the Office of the Data Protection Ombudsman worth mentioning in this context is a decision of the Deputy Data Protection Ombudsman on the Helmet libraries, which concerned the use of Google Analytics and also dealt with data transfer. Boosted by President Biden's visit to Europe in the spring, the US data adequacy decision moved forward and the European Commission published its draft adequacy decision in mid-December. The Data Protection Board gave its opinion on the matter in early 2023. The topic will certainly continue to be a central theme in data protection forums.

In addition to international data transfer, AI will probably come to the fore in the coming years, with related legislative projects being launched at both national and EU level. Legislative amendments adopted by Parliament have already set the framework for automated decision-making in an authority's decision-making process. This is a trend that I hope we can also utilise in our own operations. The screening process for pending matters introduced last year would provide a good basis for this.

Over the past year, the EDPB's dispute resolution procedure also adopted its place as a well-established form of cooperation between supervisory authorities. The EDPB issued five dispute resolution decisions over the course of the year, one of which concerned the processing of children's personal data by Meta (Instagram), which lacked an adequate legal base. Following the decision of the Board, the Irish supervisory authority imposed an administrative fine of EUR 405 million on Meta. The EDPB also issued a series of rulings on the legal base for the targeting of advertisements, which concerned Instagram, WhatsApp and Facebook.

The roll-out of the new strategy of the Office of the Data Protection Ombudsman, finalised in 2022, was started. Focus areas include cooperation in the EU, customer orientation, cooperation with stakeholders and wellbeing at work. A new vision was simultaneously created. The composition of the office was renewed in the autumn when Annina Hautala started in her position as the new Deputy Data Protection Ombudsman.

A two-year project to create a tool for SMEs was completed, and the tool was published for everyone to use and develop further. A new similar project funded by the Commission was also launched. The new project aims to improve the data protection of children.

Old dormant practices from the COVID-19 period were also revived. The regular meeting of the Nordic supervisory authorities took place in Helsinki this time. Throughout its history, one of the criteria for selecting the location of the meeting has been proximity to a body of water. Nordic meetings of supervisory authorities have been held since 1988, but there was a break due to COVID-19.

Many of the themes featured over the past year will become more significant in 2023. In the spring of 2022, the European Data Protection Board met in Vienna to discuss the improvement of its working practices. A joint statement by the supervisory authorities emphasised the importance of closer cooperation. The meeting prompted the Commission to adopt regulations complementing the General Data Protection Regulation. The focus is on streamlining cooperation between the supervisory authorities. Joint coordinated actions by the supervisory authorities as a form of cooperation were established, for example. The second coordinated action to investigate the current position of Data Protection Officers started in early 2023.

The Commission's package of data regulations will have a significant impact both in 2023 and beyond. The Commission aims to give a boost to the digital single market. Everything is built on trust, with people at the centre. The key to successful implementation is making the responsibilities of the supervisory authorities clear. The powers of the authority were also one of the focus areas for the Office of the Data Protection Ombudsman in 2022. The impact of both the renewed data regulation and the measures to streamline operations will therefore be felt in the coming years.



**Anu Talus**  
Data Protection Ombudsman



Deputy Data Protection Ombudsman  
Heljä-Tuulia Pihamaa:

# Children's data protection, patient and client data processing and other public-sector data protection issues

Like the previous year, 2022 was an extremely busy data protection year. In my remit, which mainly concerns data protection issues related to the public sector and issues processed at the national level, such as data protection questions related to social welfare and health care services, the education sector and the application of the Act on the Protection of Privacy in Working Life, we processed matters involving the exercise of the rights of the data subject, data protection notifications filed by controllers and requests for prior consultations. Questions involving matters such as the processing of children's personal

data, tracking technologies used on websites and the lawful processing of health data came up during the year.

As in previous years, social welfare and health care matters were quantitatively the largest category of matters instituted with the Office of the Data Protection Ombudsman in 2022. The most common matters instituted with the Office were personal data breach notifications and matters involving the exercise of the statutory rights of the data subject, such as requests concerning the right of access and right to erasure.

**Help is on the way for questions concerning the processing of children and young people's personal data, especially in the context of leisure activities.**

Due to the purpose of the data, orders to rectify or erase patient data or social welfare client data are in practice issued very seldom. Erasing all patient data or social welfare client data is practically impossible; for example, the erasure of diagnoses made by a health care professional cannot be ordered.

As a regulated sector, there is a clear need for official guidance in the social welfare and health care sector. We accordingly published a guide for the processing of social welfare client data in the autumn of 2022 to support controllers in their work. The guide explains matters such as the Office of the Data Protection Ombudsman's established decision-making practice. The

instructions of personal data breach notifications, first issued in 2021, were also updated with new examples on the Office of the Data Protection Ombudsman's website.

The transfer of student welfare services to the wellbeing services counties brought to light new data protection issues. Those working in the multi-sector field of student welfare are frequently faced with questions involving the disclosure of personal data. These questions also play a key role in the development of information systems in the education sector and wellbeing services counties. As clarification and instructions are needed to secure both the wellbeing of children and young people and multi-sector cooperation, we made a proposal to the Ministry of Education and Culture, Ministry of Social Affairs and Health, Finnish Institute for Health and Welfare and National Board of Education for clarifying the criteria for disclosing data and issuing national instructions on the subject. We gave several statements on reforms related to early childhood education and care and the education sector in 2022.

In late 2022, a decision of the Deputy Data Protection Ombudsman addressed the use of tracking technologies on an authority's website. As a rule, people should be able to use official online services without having data on their website visit end up in commercial use, for example. The use of tracking technologies must not convey the data subjects' personal data unlawfully to third parties. Neither may personal data be transferred unlawfully to the United States. The decision concerned the use of analytics tools such as Google Analytics.

In the field of data protection in working life, the Office of the Data Protection Ombudsman's Sanctions Board dealt with a matter involving the processing of employees' health data. The Sanctions Board imposed an administrative fine on a controller that had unlawfully stored its employees' health data in an HR system and neglected to inform its employees of the processing of their personal data.

Help is on the way for questions concerning the processing of children and young people's personal data, especially in the context of leisure activities. The two-year GDPR4CHRN project, implemented with TIEKE Finnish Information Society Development Centre and focusing on the promotion of children and young people's data protection in leisure activities, was launched in the autumn of 2022. The project is funded by the European Commission, and its primary aim is to provide information on the processing of personal data to associations that organise leisure and hobby activities for children.



**Heljä-Tuulia Pihamaa**  
Deputy Data Protection Ombudsman

## Deputy Data Protection Ombudsman Annina Hautala:

# A diverse data protection year in security and the judicial administration

I took up the post of Deputy Data Protection Ombudsman in September 2022. For my part, the final months of the year were mostly spent on getting to know my new position and the Office, as well as familiarising myself with my duties and team. This was made much easier by the professionalism and experience of my colleagues.

In my position, I took up the management of the Office of the Data Protection Ombudsman's customer service team, which mainly deals with data protection issues in the security and judicial administration. As a special feature of the position, application of the Law Enforcement Directive and its national implementing act, the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security, play a significant role in my duties.

As the year drew to a close, more and more of my unit's time was spent on parliamentary committee hearings and the preparation of statements on legislation. We were consulted on, for example, the government report on intelligence legislation. We

were also heard on a wide range of other subjects, including the proposed reform of emergency response centre legislation and the government proposal concerning personal identity codes and the procedures for issuing them.

With regard to new technologies, our statements and hearings on the government proposal for a digital identity card and the government proposal for automated decision-making in public administration merit a special mention. We should keep in mind that data protection requirements are technology-neutral. Regarding data protection in automated decision-making, we had to remind the legislator especially that data protection legislation requires that data subjects be informed in a timely manner and gives them the right to object to being subjected to automated decision-making. The discussion on data protection related to artificial intelligence solutions and automated decision-making will continue, as I feel it should, since these technologies are advancing at a considerable pace and creating new opportunities, but also risks in terms of data protection.

As in previous years, our data protection enforcement activities included planned audits of controllers. This year, these audits focused on the internal security sector. This focus was justified by the data subjects' limited opportunities to monitor the processing of their personal data in this sector themselves. The audit plan also took into account the monitoring and audits of EU information systems related to internal security in accordance with the special regulations concerning them.

Participation in the work of the European Data Protection Board's subgroups as well as the work of joint monitoring groups on the Schengen Information System (SIS II), the European Asylum Dactyloscopy Database (Eurodac) and the central EU Visa Information System (VIS) were key parts of the Office of the Data Protection Ombudsman's international cooperation.

The audits conducted in 2022 showed that controllers have taken the observations made in previous audit reports seriously and rectified shortcomings. Guidance was given to controllers and development needs pointed out based on the audits. The largest audits conducted in 2022 included those of the Visa Information System and Schengen Information System.

We made two audit visits to the Finnish Security Intelligence Service to inspect the lawfulness of their processing of personal data based on requests made by data subjects and discuss current issues.

Our unit also worked on the statements requested from the Data Protection Ombudsman for the consideration of charges. The Office issued such statements in 37 cases in 2022. The prosecutor is required to hear the Data Protection Ombudsman before bringing charges for offences such as a secrecy offence, a violation of the secrecy of communications, unlawful access to an information system, or a data protection offence, if the offence

is directed at a personal data filing system. When considering such a case, the court must give the Data Protection Ombudsman an opportunity to be heard.

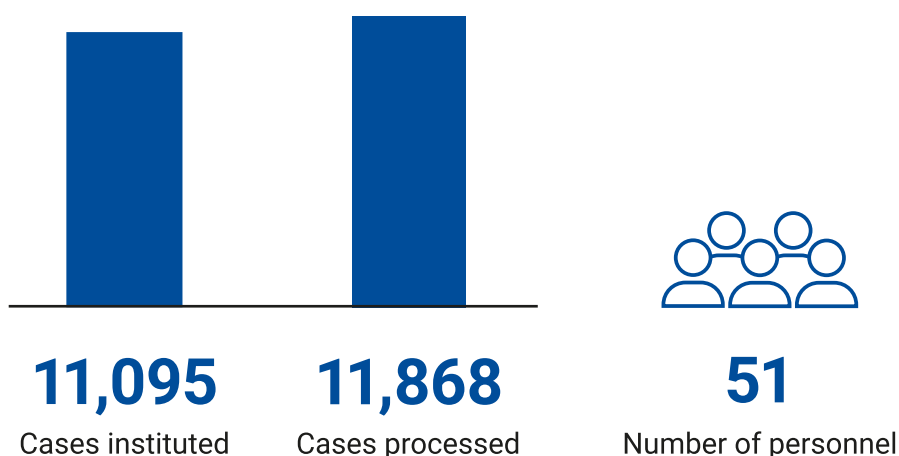
In 2022, the corrective powers of the Data Protection Ombudsman were exercised on three occasions in the security and judicial sector. In this review, I would like to highlight the decision issued in February 2022, the principal message of which was that a controller cannot use the data subject's exercise of their right of access as an information-gathering tool for the authority. The decision issued a reprimand to the controller and ordered it to cease its practices for checking the criminal records of foster parent applicants, which were in violation of the GDPR.

There have been changes in the security and judicial administration sector in the past year, and data protection practices need to be updated accordingly. These will not be the last changes going forward. The overall environment is influenced by the war in Ukraine, technological advances and Finland's internal security situation. The current situation serves as a powerful reminder of the significance of data protection.



**Annina Hautala**  
Deputy Data Protection Ombudsman

# Office of the Data Protection Ombudsman's year 2022 in figures



- 5** decisions imposing administrative fines for data protection violations
- 53** reprimands for processing measures that violated the GDPR
- 23** orders to bring personal data processing measures into compliance with the GDPR
- 11** orders to notify data subjects about a personal data breach;
- 4** cautions concerning planned processing activities that would probably violate the GDPR



**5,445**

Personal data  
breach notifications



**4**

Audits and  
audit entities



**2,801**

Calls answered by  
the telephone service



**57**

Statements on  
legislative projects



**18**

Number of times  
as the lead  
supervisory authority  
in cross-border cases

**112**

Number of times as  
a concerned super-  
visory authority in  
cross-border cases

# Focus areas of data protection activities

## Sanctions Board: Administrative fines for violations of data protection legislation

The sanctions board of the Office of the Data Protection Ombudsman is tasked with matters involving the imposition of administrative fines under the General Data Protection Regulation on controllers or processors. The Sanctions Board is made up of the Data Protection Ombudsman and two Deputy Data Protection Ombudsmen. The Board is chaired by the Data Protection Ombudsman. In 2020–2022, the Sanctions Board has imposed a total of 17 administrative fines for violations of the EU General Data Protection Regulation.

Administrative fines are one of the corrective powers available to the Office of the Data Protection Ombudsman. 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. Administrative fines cannot be imposed on public organisations, such as the central government and state-owned companies, municipalities or parishes. An administrative fine must be dissuasive, effective and proportionate.

Administrative fines were imposed on five organisations. In particular, the violations leading to administrative fines concerned issues with fulfilling the rights of the data subject and inadequate procedures for processing health data. The first administrative fine for non-compliance with an earlier order issued by the Data Protection Ombudsman was issued in the spring of 2022. The administrative fines ranged from 8,300 to 750,000 euros.

Two cases were processed in the cross-border cooperation mechanism with the Office of the Data Protection Ombudsman as the lead supervisory authority. The decisions are binding on the supervisory authorities that participated in the processing of the cases.



## In 2022, the Sanctions Board imposed administrative fines on five organisations for violations of data protection legislation.

- The Sanctions Board imposed an administrative fine of 750,000 euros on Alektum Oy for serious data protection violations. The company had regularly neglected to respond to data subjects' requests concerning their data protection rights. Neither had the company complied with its duty to cooperate with the supervisory authority.
- An administrative fine of 8,300 euros was imposed on a telemarketing company for failing to comply with the Data Protection Ombudsman's earlier order regarding the fulfilment of a data subject's right of access. The Data Protection Ombudsman had ordered the company to fulfil a customer's request to access the recording of a sales call made to the customer. This was the first administrative fine ever imposed for non-compliance with an order of the Office of the Data Protection Ombudsman.
- A publishing company was given an administrative fine of 85,000 euros for shortcomings in the implementation of data protection rights involving emails. Some of the data subjects' requests for access and erasure had been left unfulfilled due to technical problems in email forwarding. The company should have ensured that the inbox was tested, as it was the primary means of contacting the company in data protection matters.
- The Sanctions Board issued an administrative fine of 230,000 euros on Viking Line for the unlawful processing of employee health data. Among other things, the company had stored its employees' health data unlawfully in an HR system. Furthermore, some of the diagnosis information stored in the system was inaccurate, and the data had been stored for a considerable time. Shortcomings were also found in how the company informed its employees of the processing of their personal data.
- An administrative fine of 122,000 euros was imposed on a company that had processed health data without the required consent. The company had not requested specific consent for the processing of types of personal data concerning health from its users. An administrative fine was imposed for the violations, because the processing of health data was part of the company's core business.

# Renewed strategy, closer European cooperation

The Office of the Data Protection Ombudsman renewed its strategy for 2022–2025 by defining strategic focus areas, a vision and a mission for its operations.

Customer orientation, cooperation with stakeholders, European cooperation and wellbeing at work were chosen as the strategic focus areas. The new vision of the Office of the Data Protection Ombudsman emphasises the Office's role as an active proponent for responsibility in the digital environment.

The predictability and transparency of the Office of the Data Protection Ombudsman's operations and decisions are key focus areas for this strategy period. The Office will seek to reinforce its cooperation with select stakeholders and clarify its purposes and goals of stakeholder relations. The Office of the Data Protection Ombudsman aims to be a pleasant and motivational workplace that attracts and retains the best experts in data protection.

In this strategy period, the Office of the Data Protection Ombudsman will also uphold its close relations with other European data protection actors. The Office will strive to advance important issues effectively in European processes.

## Closer cooperation between data protection authorities in the EEA

In April 2022, the data protection authorities of the EU and EEA issued a joint statement that national data protection authorities were reinforcing their cooperation in the implementation of the GDPR. The statement presented the key goals and measures for more effective cooperation. Among other things, the data protection authorities

agreed on the implementation of joint inspection measures, the setting of annual priorities at the European level, and on improving the efficiency of cross-border exchanges of information. The authorities also agreed on closer cooperation in strategically significant cross-border cases between Member States.

The joint goal of the European Data Protection Board is to further harmonise the Member States' interpretation of legislation and establish the powers introduced by the enforcement and supervision of EU's new data protection regulations. In October, the European Data Protection Board delivered to the Commission a summary of administrative procedures that should be harmonised according to the Board.

## Nordic data protection authorities met in Helsinki

The data protection authorities of the Nordic countries met in Helsinki in October 2022. At the meeting, the data protection authorities of Finland, Sweden, Norway, Denmark, Iceland, Åland and the Faeroe Islands discussed Nordic cooperation and current phenomena in data protection.

The data protection authorities agreed on closer practical cooperation through sharing information and best practices, for example in the areas of children's online gaming, publicity legislation, case processing and the European health data space. In their resolution issued at the end of the meeting, the data protection authorities stressed that the enforcement of data protection regulations should not be fragmented as a result of the EU Digital Services package. The authorities also called for sufficient resourcing should the duties of the data protection authorities be increased.

## Backlog clearing and new processes

The number of cases processed by the Office of the Data Protection Ombudsman grew for a long time after the entry into force of the General Data Protection Regulation. In recent years, the number of cases instituted annually has stabilised at around 11,000. A total of 11,095 cases were instituted with the Office in 2022. The number of cases resolved exceeded the number of instituted cases by 774, i.e. roughly 11,870 cases were resolved during the year.

The Office of the Data Protection Ombudsman has been systematically clearing its backlog of cases since 2020, and this project also progressed in 2022. The original objective of the backlog-clearing project was to clear the jam of unresolved cases instituted in 2014–2018. Since then, this backlog clearing has been extended to all cases instituted with the Office.

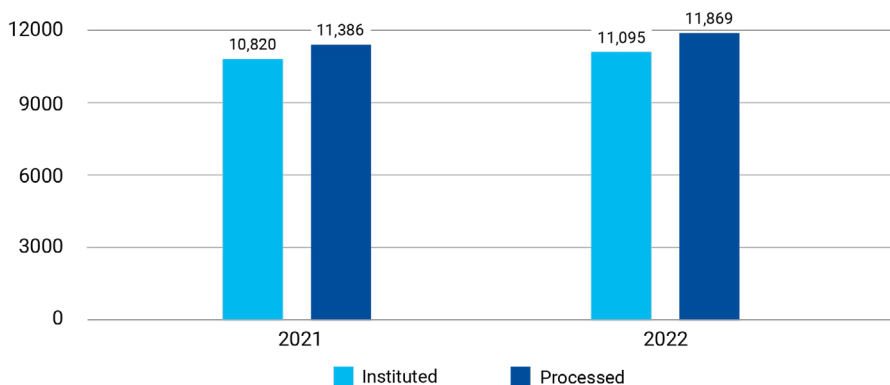
At the end of 2022, there were approximately 900 unresolved cases instituted in 2018–2020 that had been pending for more than two years.

Cross-border cases whose processing depends on another supervisory authority in the EEA constitute a significant percentage of the older unresolved cases.

The Office developed its internal procedures during the year in order to improve the efficiency of processing. A new screening process was adopted for cases involving the rights of the data subject. This screening was piloted in cases related to the health care sector, and the Office is currently evaluating the application of this model to other sectors as well.

The use of the prioritisation and screening procedure (PRISE) adopted last year and the screening process for personal data breach notifications became established practice. The personal data breach notification screening process has been found to improve the efficiency of notification processing by a significant degree. In 2022, nearly half of all cases instituted with the Office were personal data breach notifications.

Matters instituted and processed from 2021 to 2022



## Continued increase in personal data breach notifications

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

A total of 5,445 data breach notifications were filed with the Office of the Data Protection Ombudsman during the year, representing an increase of more than 660 from the previous year. The numbers of reported data breaches have increased annually and constituted nearly 50% of cases instituted. The most notifications are received from regulated sectors, such as social welfare and health care, the financial sector and the telecommunications sector.

The Office continued to employ the personal data breach notification screening procedure adopted in the previous year. The procedure has improved the efficiency and speed of notification processing and evaluation.

In the autumn, the Deputy Data Protection Ombudsman issued a reprimand to a health care provider for inadequate security measures. The

health care provider had notified the Office of the Data Protection Ombudsman of a personal data breach in which a computer case containing a laptop, some paper documents and two external hard drives had been stolen. The stolen devices contained the health and insurance data of clients, among other things. Securing the personal data stored on the laptop with a simple password was an inadequate safeguard, and the data could have been encrypted with a variety of encryption software, for example.

Organisational preparedness for personal data breaches is an important aspect of data security management and preparing for cyber incidents. Cyber incidents can involve a risk of serious personal data breaches or leaks. As part of their preparations for such incidents, organisations should ensure that, for example, system security and the notification and documentation practices for personal data breaches are in order. In terms of the technical security of personal data processing, the Office of the Data Protection Ombudsman underlines the importance of keeping software updated, access control and the adequate monitoring and logging of information systems.

The secure processing of personal data was very much on the general government agenda in 2022. The Information Management Board published the Assessment criteria for information security in public administration (Julkri) in the spring of 2022. The Information Management Board's data security section drew up the criteria in cooperation with the Office of the Data Protection Ombudsman. This is the first edition of the criteria to include a dedicated section on data protection. Use of the criteria supports organisations in the planning, implementation and evaluation of information security and the protection of personal data.

**The Office of the Data Protection Ombudsman received 5,445 personal data breach notifications in 2022.**

# Processing cross-border matters

Cross-border processing refers to the processing of personal data

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

When the processing of personal data crosses borders, the European data protection authorities monitor the processing of personal data in cooperation. A supervisory authority with overall responsibility for the processing is appointed and works together with the supervisory authorities participating in the processing of the matter. The purpose of the cooperation procedure is to achieve a binding common decision by the leading and participating authorities, as well as to ensure the consistent application of the GDPR across Member States. The European Data Protection Board publishes a [register](#) of joint decisions taken by data protection authorities.

During the year, the Office of the Data Protection Ombudsman issued two decisions in cross-border cases in which it served as the lead supervisory authority. The case concerning Viking Line was resolved in cooperation with the Swedish, Estonian and Norwegian supervisory authorities. The other case, related to a company that had processed health data without the appropriate consent, was processed in cooperation between several Member States, since the service is available in a number of countries in the EU and EEA. The Office of the Data Protection Ombudsman

**In 2022, the Office of the Data Protection Ombudsman was designated as the lead supervisory authority in 18 cases and as a supervisory authority concerned in 112 cases.**

led the investigation because the company's Finnish office is responsible for the processing of personal data. One of the complaints against the company had been instituted in another Member State.

In February, the European data protection authorities ruled that use of the Google Analytics service on a website is a violation of the GDPR. The decision was issued by the lead supervisory authority in the case, the French supervisory authority CNIL. According to the decision, the safeguards adopted by Google for the transfer of personal data via Google Analytics were inadequate.

A decision concerning Interactive Advertising Bureau Europe (IAB Europe), issued by the Belgian supervisory authority, found that IAB Europe was responsible for non-compliance with the GDPR. The decision, made in the data protection

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

authorities' cooperation mechanism, found that the Transparency & Consent Framework mechanism developed by IAB Europe did not meet the requirements of data protection regulations.

During the year, the Office created new practices for the processing of cross-border cases. The new processes clarified questions such as which factors the Office of the Data Protection Ombudsman is required to take into account when processing a case as the lead supervisory authority, and how objections made against a draft decision will be taken into account in the decision. The procedure concerning objections made against draft decisions issued by other supervisory authorities was also developed.

The European Data Protection Board issued several decisions concerning Meta Platforms

Ireland Limited in dispute-resolution proceedings in 2022. Based on the EDPB's dispute resolution decision, the Irish data protection authority imposed an administrative fine of 405 million euros on Meta in September for data protection violations in the processing of children's personal data on Instagram. The EDPB found that Meta was processing children's personal data unlawfully, without an applicable basis for processing.

In December, the EDPB issued decisions on the processing of personal data on Facebook, Instagram and WhatsApp.

The EDPB found that Meta did not have a lawful basis for processing personal data for behavioural advertising purposes on Facebook and Instagram. Using a contract as the legal basis for processing was not appropriate in connection with terms of service, since behavioural advertising is not part of these companies' core functions. In its decision based on the EDPB's decisions, the Irish data protection authority imposed 390 million euros in administrative fines on Meta. These decisions will have a far-reaching impact on the use of personal data for behavioural advertising at large.

With regard to WhatsApp, the EDPB found that a contract was not a lawful basis for processing personal data for the purpose of developing WhatsApp's service. Based on this dispute resolution decision, the Irish data protection authority imposed an administrative fine of 5.5 million euros on Meta.

In March, the EDPB adopted a new guideline for the application of Article 60 of the GDPR. The Article provides for cooperation between the lead supervisory authority and other supervisory authorities concerned. This guideline was put into practice at the Office with staff workshops, for example.

# Projects to support controllers

## The GDPR2DSM project supported SMEs in acquiring data protection expertise

The Office of the Data Protection Ombudsman's and TIEKE Finnish Information Society Development Centre's two-year, EU-funded GDPR2DSM project continued in 2022. The project supported microenterprises and SMEs in fulfilling data protection requirements and produced information and tools for ensuring data protection in companies.

The online tool developed in the project was launched on International Data Protection Day in January. Companies can use the tool to test whether their operations meet data protection requirements, determine their role in processing personal data and improve their data protection competence. In addition to the tool, other information related to data protection was also compiled on the [tietosuojaapkyrityksille.fi website](https://tietosuojaapkyrityksille.fi) to support SMEs. The source code and contents of the data protection tool were published for free use and further development.

In the spring, the project organised four regional data protection conferences in Oulu, Jyväskylä, Tampere and Turku, respectively. The project also hosted webinars in the spring and summer. The project's final conference was held in Helsinki in September, with the theme of developing the data protection competence of SMEs in a changing business environment. The project was funded by the Citizens, Equality, Rights and Values EU programme.

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

In the summer of 2022, the European Union's Citizens, Equality, Rights and Values programme

granted funding to the Office of the Data Protection Ombudsman and TIEKE Finnish Information Society Development Centre for a new project promoting the data protection of children and young people.

*GDPR4CHLDRN – Ensuring data protection in hobbies* is a two-year project aimed at improving the data protection competence of children and young people aged 13–17, their parents and clubs and associations that organise hobby and leisure activities for them. To achieve this objective, the project will draw up practical written materials and icons illustrating data protection concepts for various target groups and organise webinars and training sessions.

The project seeks to promote the realisation of data protection for children and young people, as well as inform children and young people of ways of protecting and managing their own personal data. The goal is that, in future, clubs and associations would be able to resolve issues related to compliance with data protection legislation in their activities more independently. The children and young people and their parents, on the other hand, will learn more about data protection rights and the protection of personal data.

The project was launched in August 2022, and cooperation with the Guides and Scouts of Finland, Football Association of Finland and Finnish Olympic Committee and the clubs and associations under these umbrella organisations began in September. The first public webinar was held in October, and a survey charting the data protection competence and views on the processing of personal data in hobby activities of children and young people, their parents and the staff of clubs and associations was conducted in November. In 2023, the project will continue with the preparation of materials and workshops for clubs and associations. The project will conclude in August 2024.

# International transfers of data and cloud services

When personal data is transferred outside the European Economic Area or to an international organisation, the level of protection for personal data may not correspond to the requirements of the EU General Data Protection Regulation. For this reason, a number of bases for transferring personal data have been specified in the GDPR, which can be used to transfer personal data while guaranteeing a level of data protection corresponding to EU requirements.

Various enforcement measures involving data transfers and cloud services were implemented during the year at both the national and European levels.

Together with 22 data protection authorities and the European Data Protection Supervisor, the Office of the Data Protection Ombudsman took part in the European Data Protection Board's first coordinated measure, which examined the use of cloud services in public-sector organisations. The supervisory authorities investigated the challenges cloud services pose for compliance with the GDPR. The measure was launched with a common survey for the organisations in September. The investigation targeted approximately a hundred organisations in sectors such as health care, finance, taxation, education and IT services. The Office of the Data Protection Ombudsman investigated the operations of three public-sector organisations in Finland.

In 2022, the Office of the Data Protection Ombudsman issued its first decisions setting precedents for international transfers of data. In December, the Deputy Data Protection

Ombudsman issued a decision addressing the use of tracking technologies on an authority's website. The cities of Helsinki, Espoo, Vantaa ja Kauniainen were issued a reprimand, since the website of libraries in the Helmet network had employed tracking technologies that may have conveyed data on, for example, the searches made by users to third parties. Appropriate basis for the transfer of personal data had not been defined. The Helmet.fi website used services such as the Google Analytics tool and Google Tag Manager service.

The Legal Register Centre instituted a request for a prior consultation with the Office of the Data Protection Ombudsman, since it had been unable to sufficiently mitigate the risks involved in the processing activities related to a planned intranet solution for its agencies. The Data Protection Ombudsman cautioned the Legal Register Centre that its planned processing activities were probably in violation of the GDPR. Among other things, the risks involved the transfer of data to authorities in third countries due to their right of access to information.

The 'Schrems II' judgment issued by the Court of Justice of the European Union in July 2020 (C-311/18) clarified the requirements for the legal transfer of personal data from EU and EEA Member States to third countries or international organisations. Before personal data can be transferred out of the EEA, the controller or processor must verify on a case-by-case basis whether an adequate level of data protection is guaranteed for the personal data being transferred.



In March, the European Commission and the United States came to an agreement on the creation of a new data protection framework between the EU and the United States. The new Data Privacy Framework is intended to replace the Privacy Shield arrangement annulled by the Schrems II judgment. The letter of intent on the Data Privacy Framework was implemented in US legislation by an implementation order issued by the President of the United States in October and a supplementary regulation concerning the court of appeal. The European Commission then issued a draft decision on the adequacy of data protection and submitted it to the European Data Protection Board for evaluation. An adequacy decision would permit the transfer of data from the EU and EEA to participating US companies in certain sectors without additional safeguards.

The guidelines for international transfers of data were supplemented in 2022 by an EDPB draft guideline on certifications as a data transfer tool.


**A joint measure of the European data protection authorities examined the use of cloud services in the public sector.**

## Auditing activities

In 2022, the Office of the Data Protection Ombudsman continued its systematic auditing activities, with a particular focus on internal security authorities.

The regulations on the Visa Information System and Schengen Information System stipulate that the supervisory authority must ensure that data processing in national systems is audited at least every four years in accordance with the appropriate international audit practices. Comprehensive audits of the technical environments and legal aspects of these systems were conducted in 2022. These audits were complex entities consisting of several parts. The audit results will be used to provide guidance to controllers and highlight development needs in their operations.

The use of data in the EURODAC system for law enforcement purposes was audited in accordance with the EURODAC regulation. The EURODAC system processes the fingerprints of asylum seekers and third-country nationals and stateless individuals apprehended in connection with illegal border crossings.



**The Office of the Data Protection Ombudsman conducted 4 audits and audit entities in 2022**

Audits of the National Police Board and National Bureau of Investigation's Financial Intelligence Unit were also initiated, focusing on transfers of personal data to third countries and international organisations. We made two inspection visits to the Finnish Security Intelligence Service to inspect the lawfulness of their processing of personal data based on requests made by data subjects and discuss current issues.

# Personnel and finances

## – reform of the organisation launched

The number of personnel employed by the Office of the Data Protection Ombudsman remained fairly stable from the previous year at approximately 50 employees in 2022. A total of 51 people were employed by the Office of the Data Protection Ombudsman at the end of the year. Master of Laws Annina Hautala was appointed Deputy Data Protection Ombudsman and started work in September 2022.

Three customer service teams operated in the Office of the Data Protection Ombudsman in 2022. One of them focused mainly on the private sector and cross-border matters, the second on the public sector and international matters and the third on matters related to the Data Protection Law Enforcement Directive and the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security. The Joint Functions team comprised IT senior specialists, communications and the Data Protection Officer. The Office's administrative, advisory and registry services have been centralised in the Administrative Unit. In addition, separate development teams coordinate practices and projects related to certain types of cases, such as personal data breaches, the rights of the data subject and cross-border cases.

Development needs were identified in the Office of the Data Protection Ombudsman's strategy work. The Office will seek to address these with reforms to its organisational structure and work arrangements. The reform was begun in late 2022 and will continue in 2023. The new organisation consists of a private-sector guidance and enforcement unit, public-sector guidance and enforcement unit, administrative unit and general staff.

The improvement of internal information management has been defined as the Office's key goal for the next few years. In 2022, the Office launched a deployment project for the judicial administration agencies' shared case management system.

The backlog-clearance project initiated at the beginning of 2020 was still reflected in the duties of personnel. More resources have been allocated to the processing of pending cases.

Human resources*	2020	2021	2022
Number of personnel at the end of the year	48	55	54
Person years	45.6	49.1	51.9
Absences due to illness, day(s) per person years	10.7	10.4	13.2
Average age	39.9	40.3	39.3
Education index	6.3	6.2	6.4

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

Finances of the Office of the Data Protection Ombudsman	Realisation 2020	Realisation 2021	Target 2022	Realisation 2022
Use of the operating expenses appropriation, €1,000	3,534	3,912	4,797	4,041
Total costs, €1,000	3,700	4,351	-	4,450

# Focus areas for 2023 and future developments

The aim with the European Commission's data strategy is to put the EU at the forefront of the data-driven society. The Commission has adopted several legislative proposals to implement the EU data strategy and strengthen the European data economy, including proposals for a Data Governance Act (DGA), a Digital Markets Act (DMA), a Digital Services Act (DSA), a Data Act (DA) and an Artificial Intelligence Act (AI). In addition, the forthcoming data regulation includes a proposal for a European Health Data Space and a new ePrivacy Regulation. Some of the proposals have progressed or are progressing to the national implementation stage. For some proposals, the preparation at EU level will continue in 2023.

The Office of the Data Protection Ombudsman emphasises that ensuring a consistent and clear regulatory framework is key to the roll-out of the new data regulations. The oversight of provisions on the protection of personal data should be centralised to the Data Protection Ombudsman. There is a risk that any other solution would lead to inconsistent administrative practices. The centralisation would also lead to resource and cost savings compared to decentralisation.

The AI Act is linked to the preparation of legislation on automated decision-making in public administration. In its opinion on the legislation, the Constitutional Law Committee justifiably drew attention to the transparency of information and the involvement of natural persons in automated decision-making.

The Office of the Data Protection Ombudsman has considered it important that the question of whether the administrative fines pursuant to the General Data Protection Regulation should also apply to public sector operators is investigated and assessed at the beginning of the new term of government. The Government Programme states that administrative fines for data breaches apply equally to the public and private sectors.

The public sector plays a key role in creating a responsible data economy. One of the effects of the reform would be the promotion of the proper consideration of integrated, default data protection in major system projects in the public sector. The Office of the Data Protection Ombudsman is looking forward to cooperation in the preparation of the reform.

## Focus areas of the Office of the Data Protection Ombudsman in 2023

- Data subject's rights and the special status of children
- Transparent and timely access to information
- Artificial intelligence, automated decision-making and profiling
- Support to Data Protection Officers
- New data regulations and powers of the Data Protection Ombudsman
- EU cooperation and cross-border decision-making procedure

# Matters instituted and processed from 2020 to 2022

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 2020–2022. The statistics have been compiled from the Office’s case management system at the end of the year in question.

The prior consultation (high risk) group of cases includes prior consultations due to the high residual risk, notifications required by the national legislation (Data Protection Act, section 31, subsection 3) as well as issues related to lists of high or low risk processing measures.

	2020 Instituted	2020 Resolved	2021 Instituted	2021 Resolved	2022 Instituted	2022 Resolved
<b>Tasks in accordance with the GDPR and the Data Protection Law Enforcement Directive</b>						
Prior consultation (high risk)	107	24	88	22	71	249
Statements	391	361	392	398	408	417
Codes of Conduct	3	0	1	2	0	1
Transfers of personal data	51	9	54	25	26	18
EU and international cooperation	1,108	860	811	760	1,018	1,016
Rights of the data subject	984	1,085	943	984	834	950
Supervision	1,009	950	1,139	1,145	1,063	1,069
Personal data breaches	4,275	4,139	4,786	5,056	5,446	5,663
Guidance and advice	2,116	2,921	1,650	2,037	1,176	1,441
Data Protection Officers	241	244	323	323	255	269
Board of Experts	0	0	3	4	2	2
<b>General, financial and human resource issues</b>	<b>667</b>	<b>717</b>	<b>630</b>	<b>630</b>	<b>796</b>	<b>774</b>
<b>Total</b>	<b>10,952</b>	<b>11,310</b>	<b>10,820</b>	<b>11,386</b>	<b>11,095</b>	<b>11,869</b>



OFFICE OF  
THE DATA PROTECTION OMBUDSMAN

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