



OFFICE OF
THE DATA PROTECTION OMBUDSMAN

ANNUAL REPORT
OF THE OFFICE OF THE DATA
PROTECTION OMBUDSMAN 2021

ANNUAL REPORT
OF THE OFFICE OF THE DATA
PROTECTION OMBUDSMAN 2021



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: Review of 2021	6
Deputy Data Protection Ombudsman Heljä-Tuulia Pihamaa: Guidance during the pandemic and data protection issues in an increasingly digital society.....	8
Focus areas of data protection activities.....	10
Sanctions for violations of data protection legislation.....	10
Backlog clearing and new processes	12
Processing cross-border matters	13
The powers and procedures of the Office of the Data Protection Ombudsman ...	14
Growth in personal data breaches continued	15
Supporting controllers in ensuring data protection	17
International transfers of data	18
Auditing activities	19
Personnel and finances.....	20
Matters instituted and processed from 2019 to 2021.....	21

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.

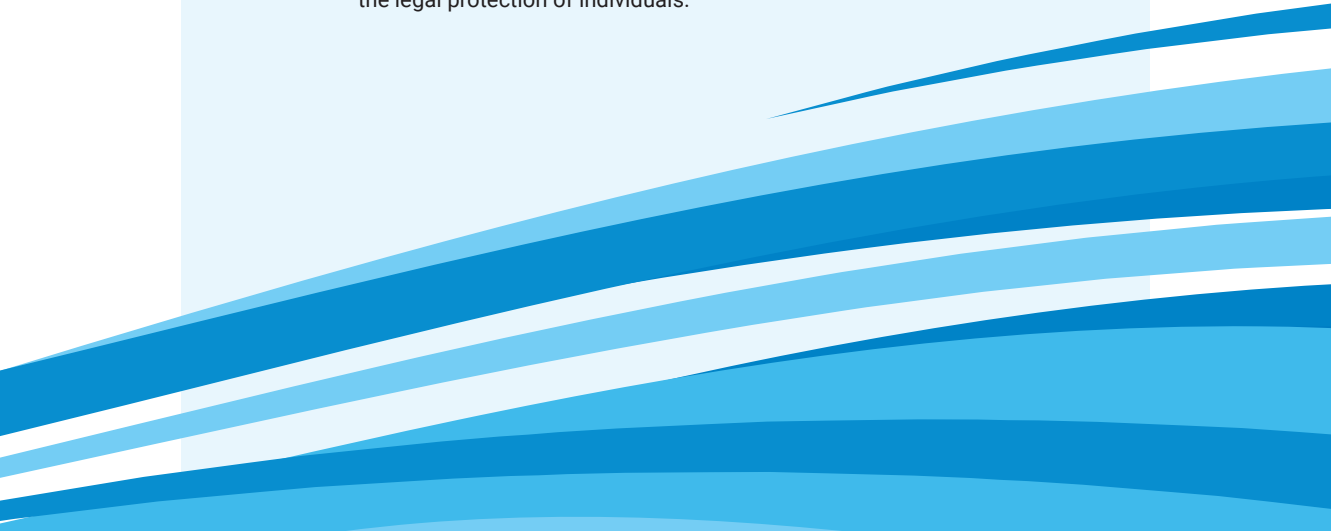
The Office of the Data Protection Ombudsman promotes awareness of the rights and obligations related to the processing of personal data, imposes administrative sanctions for violations of the General Data Protection Regulation of the EU, if necessary, carries out investigations and inspections and issues statements on legislative and administrative reforms. The Data Protection Ombudsman cooperates with the data protection authorities of other countries and represents Finland on the European Data Protection Board (EDPB).

In 2021, the Data Protection Ombudsman was Anu Talus. Jari Råman and Heljä-Tuulia Pihamaa served as Deputy Data Protection Ombudsmen. Master of Laws Pihamaa was appointed Deputy Data Protection Ombudsman in January 2021 and start work in March. The Data Protection Ombudsman and Deputy Ombudsmen are appointed by the government for terms of five years.

Objectives of the Office of the Data Protection Ombudsman

- We will promote the citizens' right to the protection of privacy and trust in the transparency of personal data processing in an increasingly digital society.
- We will successfully implement the objectives and effects of the data protection reform in national legislation and the activities of authorities.
- We will deter personal data breaches.
- We will promote the awareness of citizens, controllers and data processors of their rights and obligations related to data protection.
- We will promote the creation of a single digital market within the EU.

Mission: Data protection is a success factor

- For private individuals, more comprehensive protection of personal data and the opportunity to manage their own data.
 - For companies, a prerequisite of success and a reputation factor resulting from responsible operations.
 - For the authorities, a part of responsibility and reliability as well as the legal protection of individuals.
- 

Data Protection Ombudsman Anu Talus: Review of 2021

The year 2021 was still defined by the coronavirus. In January, the international Data Protection Day was nevertheless celebrated for the second time, this time in the form of a remote seminar. A remote seminar does not provide the opportunity to meet colleagues and network among one's peers but is easier to attend, also for those not living in Helsinki.

In January, the Government appointed the second Deputy Data Protection Ombudsman Heljä-Tuulia Pihamaa, to her position, and Pihamaa started work in March 2021.

The numbers of cases instituted had been growing for several years running, but this growth stopped in 2021. Just under 11,000 cases were instituted in 2021, as was the case in 2020. The Office continued the systematic backlog-clearing project initiated in 2020, which has successfully addressed the backlog in case processing.

The Office of the Data Protection Ombudsman issued a number of decisions and statements and was heard by various parliamentary committees. Questions involving the rights of the data subject, especially the right of access, were a recurring theme in complaints. Several decisions also gave precedents on data minimisation and privacy by design. The rights of the data subject are implemented best when data protection is included in the design of new technologies, platforms and

applications from the ground up. We will continue to draw attention to this obligation laid down in the GDPR going forward as well. The connections between data protection and data security, the secure processing of data, and neglect were also emphasised in the Ombudsman's decision-making practice.

The strategy update of the Office of the Data Protection Ombudsman started with a survey for stakeholders and citizens, which was completed in May. Its results showed that the Office's expertise and reliability is appreciated, but its operations could be more customer-oriented.

To support controllers, we published a guideline for impact assessments in December. Implementation of the Commission-funded GDPR2DSM project, launched in the autumn of 2020 and aimed at SMEs and implemented in cooperation with TIEKE Finnish Information Society Development Centre, also continued in 2021. To provide base data for the project, we charted the data protection challenges and needs of SMEs in the spring. Tool development workshops began in the summer, and the project's webinar series were kicked off in the autumn.

The routines of Sanctions Board proceedings became further established in 2021. In proceedings involving the hearing of the controller, the controller is reserved an opportunity to be heard

before the matter is discussed by the Sanctions Board. During the hearing, the facts of the matter and the referendary's preliminary assessment are presented to the controller. In 2021, the Administrative Court issued its first judgments stating that this procedure is in compliance with the Administrative Procedure Act.

The Sanctions Board imposed administrative fines on a total of seven controllers during the year. Administrative fines were imposed on a controller that had made robot calls without the appropriate consent as well as on a private parking control company that had processed personal data illegally, among others. The matter involving Psykoterapiakeskus Vastaamo was brought to a conclusion at the Office of the Data Protection Ombudsman in a Sanctions Board hearing that imposed an administrative fine on Vastaamo. Administrative fines were also imposed on a university of applied sciences for the unnecessary processing of employee location data and on the Finnish Motor Insurers' Centre for the unnecessarily extensive collection of patient records.

Other significant decisions made in 2021 included a reprimand issued to the police for the use of Clearview AI facial recognition technology, as well as a decision finding that the tax lists published by the media constitute the processing of personal data for journalistic purposes. A reprimand was issued to a company that relayed its customers' personal data to the personal phones of employees via WhatsApp.

The European Data Protection Board (EDPB) also continued working on a remote basis. Significant decisions made by the EDPB in 2021 included a binding decision issued in a dispute resolution procedure in a matter concerning WhatsApp and the first decision issued through the urgency


procedure. For its part, the Office of the Data Protection Ombudsman issued its first decision as the lead supervisory authority in a cross-border procedure.

International transfers of data remained a significant topic in international data protection forums in 2021 as well. The European Commission issued two separate decisions on the adequacy of data protection in Britain. One of the decisions was the first of its kind to be issued under the Data Protection Law Enforcement Directive. Transfers of data to third countries will remain a relevant topic in future as well as frameworks and guidelines are being updated.



Anu Talus

Data Protection Ombudsman



Deputy Data Protection Ombudsman Heljä-Tuulia Pihamaa: Guidance during the pandemic and data protection issues in an increasingly digital society

I took up the post of Deputy Data Protection Ombudsman in March 2021. My task is to lead one of the Office of the Data Protection Ombudsman's customer service teams, which mainly deals with 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.

Like the year before, 2021 was still defined by the coronavirus pandemic. We issued expert statements on legislative bills and responded to inquiries and complaints involving the coronavirus.

A number of expert statements on legislation projects related to the health and social services reform were issued. 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. Nearly 30 per cent of all matters instituted in 2021 involved social welfare and health care, and personal data breach notifications constituted a significant portion of these matters. The conditions for notifying the authorities are met often in sectors processing special categories of personal data, which partly explains the large number of notifications from the social welfare and health care sector in comparison to other sectors.

A data protection survey conducted in cooperation with the Social Insurance Institution of Finland (Kela) and the National Institute for Health and Welfare showed that there is a need for concrete instructions on personal data breach notification procedures in the social welfare and health care sector. To respond to this need, we issued guidelines on the personal data breach notification duty, especially tailored for social welfare and health care operators, in late 2021.

We hope that the guidelines will also be of help in other sectors. It is evident that guidance in the area of personal data breach notifications will be required going forward as well, so the guidelines will be updated in 2022.

Like society in general, the education sector is increasingly digitalised, and the phenomenon applies to all education providers and educational institutions.

It can be said that the education sector took a 'digital leap' during the coronavirus pandemic, and teaching quickly moved to digital environments. These developments were also reflected in the education sector issues instituted with the Office of the Data Protection Ombudsman, many of which concerned data protection questions related to applications used in teaching. Those adopting digital services for educational use need to be able to take other regulations concerning teaching into account in addition to personal data processing legislation. For this reason, we proposed that the National Board of Education draw up guidelines for the adoption of teaching applications in the education sector. It is our hope and objective that this work, which requires cooperation, will progress in 2022 and questions involving the processing of students' personal data will be properly addressed in the use of teaching applications.

We sought to ensure compliance with data protection legislation in Finnish working life through cooperation with stakeholders, such as the occupational safety and health authorities, as well as by issuing statements on legislative projects and central government guidelines. During the coronavirus pandemic, the question

"Are employers allowed to process data on their employees' coronavirus vaccinations?" was momentarily one of the questions most frequently asked from the Office. We sought to meet the need for information during the pandemic by publishing general guidelines on the Office website.

The Office also participated in the tripartite preparations for the required amendments to the Act on the Protection of Privacy in Working Life, which are aimed at mitigating the challenges that have arisen in the application of the law, among other things. The work will continue in 2022.



Heljä-Tuulia Pihamaa
Deputy Data Protection Ombudsman

Focus areas of data protection activities

Sanctions for violations of data protection legislation

The Sanctions Board of the Office of the Data Protection Ombudsman is tasked with imposing administrative fines under the GDPR 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. The Board started operations in the autumn of 2019 and imposed its first administrative fines in May 2020.

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. The Sanctions Board made one decision in 2021 in which an administrative fine was waived. This decision concerned a subcontractor that implemented direct marketing calls on behalf of a controller in the role of personal data processor. Imposing a fine would have been

effective and dissuasive, but not proportionate in view of the seriousness of the violation. In its assessment, the Board took into account matters such as the company's turnover and pending bankruptcy filing.

In 2021, the Office of the Data Protection Ombudsman issued

- 7 decisions imposing administrative fines for data protection violations;
- 29 orders to notify data subjects about a personal data breach;
- 36 orders to bring personal data processing measures into compliance with the GDPR; and
- 59 reprimands for processing measures that violated the GDPR.

In 2021, the Sanctions Board imposed administrative fines on seven organisations for violations of data protection legislation.

- ParkkiPate Oy was ordered to pay an administrative fine of EUR 75,000 for data protection violations. These violations involved, among other things, failure to fulfil the rights of the data subject and shortcomings in the limitation of data storage periods. The company also regularly processed personal data more extensively than necessary for identification purposes.
- A magazine publisher was ordered to pay an administrative fine of EUR 8,500 for direct marketing without consent. The robot calls had not been designed to ensure that data subjects were able to exercise their data protection rights. Neither had the controller or the subcontractor performing the direct marketing calls on its behalf drawn up a processing agreement for the implementation of the direct marketing.
- An administrative fine of EUR 25,000 was imposed on a higher education institution for data protection violations connected to processing of location data. The employer processed its employees' location data unnecessarily and without legal grounds, using a mobile application intended for recording working hours.
- In December 2021, the Sanctions Board imposed an administrative fine of EUR 608,000 for data protection violations on Psykoterapiakeskus Vastaamo Oy. Vastaamo had neglected basic procedures of secure processing and duties related to the reporting of personal data breaches. Vastaamo should have notified both the Data Protection Ombudsman and its customers of the personal data breach without delay since it caused a high risk to those affected by the data breach. Shortcomings were also found in the documentation required to demonstrate accountability.
- The Sanctions Board imposed an administrative fine of EUR 5,000 on a medical clinic for neglecting the rights of the data subject. The clinic had not fulfilled a customer's right to access their patient records appropriately and its practices for implementing the rights of the data subject were insufficient. Neither had the clinic clearly indicated for which data it was serving as a controller.
- A travel agency was ordered to pay an administrative fine of EUR 6,500 for shortcomings in the security of processing and implementation of the rights of the data subject. The travel agency had used an unencrypted network connection for visa applications and stored forms containing personal data on an open net server.
- The Finnish Motor Insurers' Centre was ordered to pay an administrative fine of EUR 52,000 for the unnecessary extensive collection of patient records. The Office of the Data Protection Ombudsman investigated the Finnish Motor Insurers' Centre's practices for requesting patient records from health care units for the processing of claims. The controller had systematically requested the full patient records of claimants instead of restricting their requests to necessary data.

Backlog clearing and new processes

The number of cases processed by the Office of the Data Protection Ombudsman has grown each year since the entry into force of the GDPR. In 2021, the number of cases instituted with the Office stabilised at the level of 2020 with 10,816 cases. The Office resolved 519 cases more than were instituted in 2021, 11,380 in total.

The Office has been systematically clearing its backlog of cases since 2020, and this project also progressed in 2021. The original objective of the backlog-clearing project was to clear the jam of unresolved cases instituted in 2014–2018.

At the beginning of 2021, a total of 427 such ‘old cases’ instituted in 2014–2018 remained unresolved. At the end of 2021, the number had been brought down to 207. Of this number, 153 constituted matters processed in international procedures and dependant on the actions of the data protection authorities of another state.

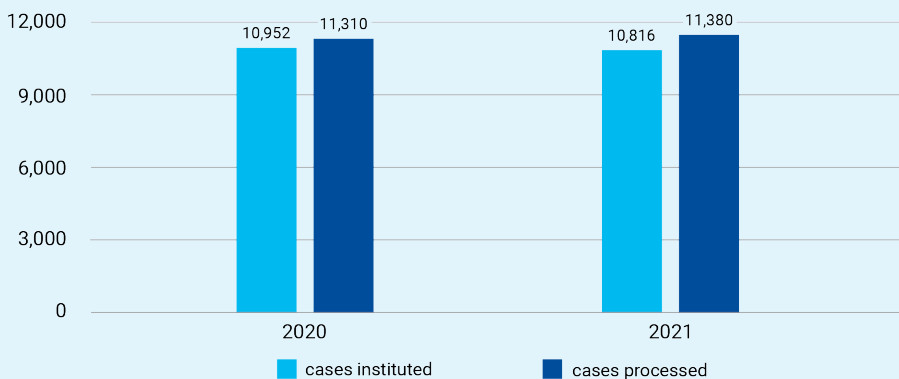
In addition to the old cases, the backlog clearing project also resolved newer cases instituted in 2019–2021. At the end of 2021, there were a

total of 4,886 pending cases instituted in 2019–2021. At the end of the year, this number had been reduced by 537.

The Office developed internal procedures for improving the efficiency of case processing. A new procedure for the prioritisation and screening of instituted cases (PRISE) was adopted in the summer with the objective of harmonising case-processing practices and ensuring the equal treatment of customers. The new procedure facilitates employee time management and the systematic allocation of resources.

Reports of personal data breaches make up 40 per cent of all cases instituted with the Office of the Data Protection Ombudsman. In the autumn, the Office adopted a new screening process for personal data breach notifications, with the objective of improving the efficiency of processing and facilitating follow-up action. This internal screening procedure complements the EDPB’s guidelines on the processing of personal data breach notifications.

Matters instituted and processed in 2020–2021



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 EDPB publishes a [register](#) of joint decisions taken by data protection authorities.

The Office of the Data Protection Ombudsman issued its first decision as the lead supervisory authority in a cross-border case in 2021. The case involved a car dealership that had not provided the information required under data protection regulations to a customer who wanted to exercise their right of access. The data included recorded telephone calls, for example. The dealership's Finnish office was responsible for the processing of the personal data.

In July, the EDPB issued a decision concerning WhatsApp Ireland Limited in a dispute resolution proceeding. The decision concerned an investigation by the Irish supervisory authority into whether WhatsApp was informing its users

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

of the processing of their personal data in a transparent manner. The case was processed in a dispute resolution proceeding, since the Irish data protection authority dismissed the objections made by the participating data protection authorities on the draft decision. The Irish data protection authority had found serious data protection violations concerning transparency in WhatsApp's operations.

In addition, the EDPB issued its first decision under the urgency procedure. The decision concerned the request of Hamburg's supervisory authority for adopting urgent measures against Facebook Ireland Limited because of changes to the terms of service of the WhatsApp instant messaging service. The EDPB nevertheless found that the conditions for an urgent procedure were not met and asked the Irish supervisory authority for more information on how Facebook is processing the data of European WhatsApp users.

The Office of the Data Protection Ombudsman also developed its own practices in the processing of cross-border cases during the year.

The powers and procedures of the Office of the Data Protection Ombudsman

Three Administrative Court decisions on appeals against administrative fines were given during the year. According to the Administrative Court, the process leading to the imposition of an administrative fine fulfilled the conditions of the Administrative Procedure Act in the cases in question.

The first Administrative Court decision, issued in May, applied to decisions made by the Data Protection Ombudsman and Sanctions Board in 2020, which the controller had demanded to be reversed. The Administrative Court found that the administrative fine had been imposed on appropriate grounds.

In its second decision, the Administrative Court overturned a Sanctions Board decision imposing an administrative fine on Posti for data protection violations. The Data Protection Ombudsman's decision concerning Posti was upheld.

In addition, the Administrative Court reduced the administrative fine imposed on Taksi Helsinki in the spring of 2020 and overturned one of the orders issued in the decision. The appeals were dismissed in other respects. The decisions are not final, and some of the questions are awaiting the opinion of the Supreme Administrative Court.

Administrative Court decisions issued in the spring of 2021 clarified the interpretation of consent to the use of cookies and powers in supervisory matters involving cookies. The Administrative Court overturned two decisions by the Finnish Transport and Communications Agency (Traficom) concerning ways to ask for users' consent to the use of cookies on websites. At the same time, the Court found that Traficom is the competent

authority with regard to the supervision of consent for the use of cookies. Following these Administrative Court decisions, the Office of the Data Protection Ombudsman transferred complaints concerning consent for the use of cookies to Traficom.

The decisions of the Administrative Court were in line with the Office of the Data Protection Ombudsman's established policy regarding the requirements for consent to the use cookies. Consent to the use of cookies must be obtained in accordance with the GDPR's provisions concerning consent. These requirements were taken into account in Traficom's new cookie guidelines published in the autumn of 2021, which were prepared in consultation with the Office of the Data Protection Ombudsman. The Administrative Court also found that Traficom must ask the Office of the Data Protection Ombudsman for a statement on the interpretation of consent under the GDPR.

The Deputy Chancellor of Justice started an investigation into the case-processing practices of the Office of the Data Protection Ombudsman in 2020 and gave his decision at the end of 2021. The Office of the Data Protection Ombudsman issued a report to the Deputy Chancellor of Justice on matters such as case processing times, the processing stages of old pending cases and the impact of measures adopted. The Deputy Chancellor of Justice also conducted a legality audit of the Office.

According to the Deputy Chancellor of Justice, the Office of the Data Protection Ombudsman's development measures look promising and the case backlog has almost been cleared. However, the improved case processing situation is at risk of taking a turn for the worse if the Office does not have access to sufficient human resources.

Growth in personal data breaches continued

Personal data breach notifications constitute the largest single category of cases instituted with the Office of the Data Protection Ombudsman. A total of 4,785 data breach notifications were filed with the Office during the year, representing an increase of more than 500 from the previous year. The numbers of reported data breaches have increased annually and have risen to 44% 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.

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. Organisations have been subject to this duty to notify since May 2018.

The Office has noted that there are differences in the identification and processing of data breaches between sectors. A need for clarifying instructions on reporting personal data breaches has been identified in the social welfare and health care sector in particular. The Office receives the greatest number of personal data breach notifications from the social welfare and health care sector.

In order to respond to this need, the Deputy Data Protection Ombudsman sent social welfare and health care operators a guidance letter clarifying the duty to notify. This guidance sought to increase awareness and understanding of personal data breaches and the statutory obligations related to them, as well as to harmonise reporting practices in the sector. Examples of notification obligations in various situations were compiled both in the letter and on the Office website.

The duty to notify was also a key theme at the European level. The EDPB drew up guidelines compiling examples of personal data breach notifications to support controllers. The guidelines give practical recommendations for situations in which an organisation is required to notify the supervisory authority and data subjects of a personal data breach.

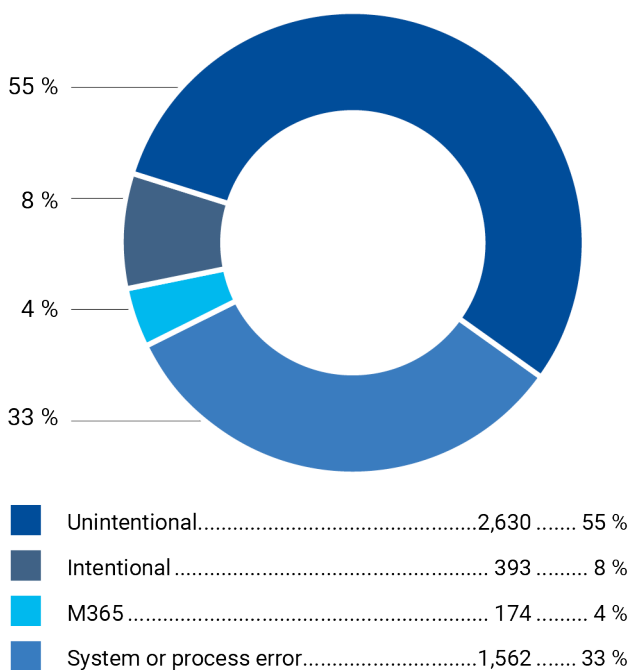
In November, the Office supplemented its instructions with regard to the retention of log data from the duration of a personal data breach committed against the information system. Log data are also included in the documentation obligation concerning personal



data breaches. The supervisory authority must be able to verify the controller's compliance with its notification duties from the documentation. The authority can request access to log data for the purposes of processing a personal data breach notification.

The Office of the Data Protection Ombudsman improved the efficiency of its internal processing of personal data breach notifications during the year. Among other things, the Office adopted a new screening procedure for expediting processing.

Personal data breaches by type in 2021



Supporting controllers in ensuring data protection

The GDPR2DSM project supports SMEs in acquiring data protection expertise

The Office of the Data Protection Ombudsman and TIEKE Finnish Information Society Development Centre were granted 2020 EU funding for the [GDPR2DSM project](#) aiming to develop an easy-to-use data protection tool for SMEs in cooperation with the companies. The tool will allow companies to increase their data protection expertise, assess the current state of their practices and get tips for improving their level of data protection.

The project was launched in the spring of 2021 with a survey charting the data protection needs and challenges of the companies. The survey was taken by approximately 350 people, most of whom represented retail companies employing less than five people. The answers showed that familiarity with the GDPR was fairly high, but its practical application was felt to be challenging.

Co-development of the tool with the companies started with a workshop for 30 participants held in June. The first version of the tool was published in October.

As part of the project, the Office of the Data Protection Ombudsman and TIEKE held free webinars on data protection for SMEs in cooperation with partners. We organised a total of fourteen webinars on themes requested by the companies during the year. The use of cookies on websites and the latest administrative fine practices in Finland and broad were particularly interesting topics for the companies.

Development of the data protection tool and events around the project will continue in 2022. The project is funded by the Citizens, Equality, Rights and Values EU programme.

Instructions for data protection impact assessments

In the spring, the Office of the Data Protection Ombudsman drew up instructions for data protection impact assessments to support controllers. We asked for feedback on the draft and developed the instructions based on that feedback over the course of the year. The final instructions were published in December 2021.

The instructions were accompanied by a simple Excel record tool, which controllers can use when making impact assessments if they wish. Where

applicable, the instructions can also be used for the impact assessment under the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security.

The purpose of the data protection impact assessment is to identify and mitigate the risks related to processing personal data, as well as to generate material that can be used to demonstrate compliance with data protection regulations.

International transfers of data

The level of protection of personal data guaranteed by the GDPR can decrease when personal data is transferred out of the European Economic Area or to an international organisation. 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.

The instructions concerning the transfer of personal data were clarified and updated during the year. In particular, 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.

Significant updates were made to the bases for transfer during the year. In June, the European Commission adopted the updated standard contractual clauses (SCCs) for the transfer of data to third countries. The transition period for implementing the updated SCCs will expire on 27 December 2022. In addition, the European Commission made two decisions in June

regarding the adequacy of data protection in the UK, by virtue of which transfers of personal data between EEA countries and the UK can continue after the post-brexit transition period.

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. If the basis for transfer being used does not guarantee an adequate level of protection by itself, it can be supplemented with various additional safeguards in certain situations. In June, the EDPB published the final version of its recommendations for supplementary measures, which help assess the need for additional safeguards and choose the safeguards appropriate to the circumstances.

The guidelines issued to authorities were also clarified in the wake of the Schrems II judgment, and the data protection authorities' responsibility for the supervision of international transfers of data was emphasised. The Office of the Data Protection Ombudsman announced in the autumn that it would enhance the supervision of transfers of personal data.

Auditing activities

The supervision of the lawfulness of the processing of personal data by the authorities competent by virtue of the Act on the Processing of Personal Data in Criminal Matters was characterized by the use of facial recognition technology and camera technology.

In addition to the Finnish Defence Forces and the police, which are the government controllers with the largest number of personnel, this area of responsibility of internal security also includes the Finnish Customs, the Finnish Border Guard, rescue services, activities of the Emergency Response Centres, immigration administration as well as courts of law, the National Prosecution Authority as well as the Criminal Sanctions Agency.

The Office of the Data Protection ombudsman continued to carry out its planned audit activities of internal security authorities in 2021. The Deputy Data Protection Ombudsman conducted a total of 8 audits of authorities of internal security during the year. Subjects of these audits included the National Police Board, the Finnish Defence Forces, the Ministry of the Interior and two police departments. In addition, inspections were carried out on the private security sector, the immigration administration and the National Prosecution Authority.



Personnel and finances

Number of personnel increased, a new deputy ombudsman was appointed

The number of personnel employed by the Office of the Data Protection Ombudsman increased in 2021. A total of 55 people were employed by the Office of the Data Protection Ombudsman at the end of 2021.

Three customer service teams operate in the Office of the Data Protection Ombudsman. As a rule, one of them focuses 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 Office's administrative, advisory and registry services have been centralised in the Administrative Unit. The Joint Functions team includes the IT senior specialists, communications and the Data Protection Officer. In addition, separate development teams

coordinate practices and projects related to certain themes, such as personal data breaches, the rights of the data subject and impact assessments.

Master of Laws Heljä-Tuulia Pihamaa was appointed Deputy Data Protection Ombudsman and started work in March 2021. As Deputy Data Protection Ombudsman, Pihamaa leads the customer service team focusing on the public sector and national cases.

With the persistence of COVID-19 restrictions and the remote work order, remote work practices and digital ways of working became established in the day-to-day operations of the Office.

The backlog-clearance project initiated at the beginning of 2020 was still reflected in the personnel of the Office. The contribution of fixed-term 'backlog clearers' has been increasingly allocated to the processing of pending cases since 2020.

Human resources	2019	2020	2021
Number of personnel at the end of the year	46	48	55
Person years	40.6	45.6	49.1
Absences due to illness, day(s) per person years	11.5	10.7	10.4
Average age	41.6	39.9	40.3
Education index	6.3	6,3	6,2

Finances of the Office of the Data Protection Ombudsman	Realisation 2019	Realisation 2020	Target 2021	Realisation 2021
Use of the operating expenses appropriation, €1,000	3,179	3,534	4,597	3,912
Total costs, €1,000	3,862	3,700	-	4,351

Matters instituted and processed from 2019 to 2021

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 2019–2021. The statistics have been compiled from the Office's case management system at the end of the year in question.

The case management groups of the Office of the Data Protection Ombudsman changed in May 2018 with the reform of the data protection legislation. Most of the cases have been recorded under tasks in accordance with the EU GDPR and the Data Protection Law Enforcement Directive starting from 25 May 2018.

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.

	2019 Instituted	2019 Resolved	2020 Instituted	2020 Resolved	2021 Instituted	2021 Resolved
Tasks in accordance with the GDPR and the Data Protection Law Enforcement Directive (groups 80–210)	9,292	7,516	10,233	10,165	10,130	10,672
Prior consultation (high risk)	45	8	107	24	88	22
Statements	206	215	391	358	385	390
Codes of Conduct	1	1	3	0	1	2
Transfers of personal data	78	68	51	9	54	25
EU and international cooperation	1,085	831	1,091	825	793	744
Rights of the data subject	870	496	984	1,085	943	984
Supervision	669	180	1,009	943	1,139	1,140
Personal data breaches	3,840	3,620	4,275	4,139	4,786	5,056
Guidance and advice	2,014	1,481	2,081	2,538	1,615	1,982
Data Protection Officers	483	616	241	244	323	323
Board of Experts	1	0	0	0	3	4
General issues (groups 01–29)	584	551	667	720	636	636
General, financial and human resource issues	580	545	667	717	630	630
Statements on e.g. administrative reforms	4	6	0	3	6	6
International matters (groups 30–39)	26	36	17	35	18	16
European Union	19	22	16	23	14	13
Other international cooperation with data protection authorities	6	7	0	2	1	1
Other international issues	1	7	1	10	3	2
Ex ante control and guidance by the Data Protection Ombudsman (groups 40–49)	100	345	35	390	35	60
General guidance	87	100	33	33	34	34
Enquiries and requests for guidance by controllers	1	73	0	130	0	7
Processing of personal data with IT within the scope of the notification obligation	1	61	0	1	0	1
Requests for information by the Data Protection Ombudsman	11	10	0	6	0	4
Enquiries and requests for measures submitted by data subjects	0	101	2	220	1	14
Orders of the Data Protection Ombudsman and other ex post control (groups 50–59)	0	0	0	0	1	2
Statements to the prosecutor and courts of law	0	0	0	0	1	1
Applications to the Data Protection Board	0	0	0	0	0	1
Unclassified	0	1	0	0	0	0
Total	10,002	8,449	10,952	11,310	10,820	11,386

