



OFFICE OF
THE DATA PROTECTION OMBUDSMAN

ANNUAL REPORT
OF THE OFFICE OF THE DATA
PROTECTION OMBUDSMAN 2020

ANNUAL REPORT
OF THE OFFICE OF THE DATA
PROTECTION OMBUDSMAN 2020



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: 2020, a year of reforms	6
Deputy Data Protection Ombudsman Jari Råman: Audits in the time of COVID-19 and questions of facial recognition technology in the field of internal security	8
Focus areas of data protection activities	10
The Office of the Data Protection Ombudsman imposed administrative fines for the first time	10
Appointment of the Expert Board	12
Measures to clear the backlog	13
Processing cross-border matters	14
Auditing activities	15
The number of personal data breaches continued to increase	16
Staff and finances – new organizational structure established, changes in the assembly of ombudsmen	18
Matters instituted and processed from 2018 to 2020	19

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 audits 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).

Reijo Aarnio was the Data Protection Ombudsman until the end of October 2020. Anu Talus was appointed as the Data Protection Ombudsman as of the beginning of November when Aarnio retired after a long service in the office. Before her appointment as Data Protection Ombudsman, Talus acted as the Deputy Data Protection Ombudsman. Jari Råman is the second Deputy Data Protection Ombudsman. The Data Protection Ombudsman and Deputy Ombudsmen are appointed by the government for terms of five years.

Goals of the Office of the Data Protection Ombudsman for 2019–2022

- 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 take preventive action to 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 development of a single digital market within the EU.

Mission: Data protection is a success factor

- More comprehensive protection of personal data for private individuals and the opportunity to manage their own data.
 - Prerequisite of success for companies and a reputation factor resulting from responsible operation.
 - A part of responsibility and reliability as well as the legal protection of an individual for the authorities.
- 

Data Protection Ombudsman Anu Talus: 2020, a year of reforms

Data Protection Day was celebrated for the first time in January 2020, in an event co-hosted by Alma Talent. The event proved to be a success, and the goal is to establish the Data Protection Day as an annual event.

The Data Protection Day later proved to be one of the last opportunities to meet international colleagues. The year was marked by the COVID-19 pandemic both in Finland and internationally. The Office of the Data Protection Ombudsman provided guidance on several questions related to COVID-19 on its homepage. The office relocated to new facilities during the spring of the first year of the pandemic in 2020, which came with its challenges.

Although the pandemic has tested the society in many ways, it has been delightful to perceive how data protection questions were kept a priority in Finland's measures against COVID-19. It has been said that the Finnish COVID-19 debate has been dominated by judicialisation, but from the data protection perspective, this is only positive. The Koronavilkku application, intended to monitor exposure to the virus, was also developed in the framework of data protection policy.

The number of matters instituted with the Office of the Data Protection Ombudsman continued to increase. With the entry into force of the EU

General Data Protection Regulation in 2018, the number of matters instituted multiplied, and the processing became congested. In early 2020, the Office started a systematic clearance of this backlog. This project has progressed as scheduled, but at the same time, the number of instituted matters continued to increase. In 2020, a total of 937 more matters were instituted than in the previous year. Notifications of data breaches accounted for more than one third of all instituted cases in 2020. An initiative to increase and boost the efficiency of the processing of data breach notifications was also launched in 2020.

The European Commission submitted an evaluation and review of the General Data Protection Regulation in May 2020, two years after its entry into force. The Commission report was drafted during Finland's Presidency of the Council of the European Union. The report states that most of the goals of the legal reform have been achieved, and that new legislation has improved citizens' rights. However, the report suggests that the need to make the harmonisation of the application of legislation more efficient continues to exist.

Last year was also a time for major decisions. The Sanctions Board of the Office of the Data Protection Ombudsman imposed its first administrative fines for breaches of data

protection legislation. A total of five rulings on administrative fines were issued. Four of these were appealed in the Administrative Court. The largest fine imposed by the Sanctions Board was 100,000 euros.

The Court of Justice of the European Union issued some significant rulings on personal data protection during the year. In July, the Court of Justice of the European Union gave a decision in the case known as Schrems II (C-311/18). The judgment invalidated the Privacy Shield system and remodified the framework of data transfer into third countries. The European Data Protection Board gave its first conclusive dispute resolution decision in a case against Twitter. The Irish data protection authority announced its decision based on the dispute resolution decision in December and imposed a fine of 450,000 euros on the company.

The surge of activity in the field of data protection continued in the autumn. The Office of the Data Protection Ombudsman and TIEKE, the Finnish Information Society Development Centre, received Commission funding for the development of a tool for SMEs to reach a data protection standard set by the GDPR. The project was launched in the latter part of the year and will last approximately two years.

The retirement of Reijo Aarnio, who served in the post of Data Protection Ombudsman for a long time, was celebrated in the autumn.

At the time of Reijo Aarnio's retirement, the most extensive breach of data protection of all time was revealed in Finland. The Psychotherapy Centre

Vastaamo filed a notification of a data breach with the Office of the Data Protection Ombudsman on 21 October 2020. In this context, other questions relevant to the protection of personal data, such as the preconditions of processing the personal identity code, were highlighted in discussion.

When looking at the most important events of last year, I cannot help but conclude that the year was full of major changes, great achievements in development, data protection actions, and even surprises. This will also be true for the year to follow.



Anu Talus

Data Protection Ombudsman

Deputy Data Protection Ombudsman
Jari Råman:

Audits in the time of COVID-19 and questions of facial recognition technology in the field of internal security

In 2020, data processing by the authorities competent by virtue of the Act on the Processing of Personal Data in Criminal Matters was, for the first time, supervised in accordance with a new audit plan. The supervision measures were particularly characterized by the extended use of facial recognition 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.

Audits are one means of completing the Office of the Data Protection Ombudsman's supervisory tasks. With the implementation of the first audit plan of the new form, it was detected that the

audits clearly provide added value, even though the measures take up a lot of resources from other tasks of the Office of the Data Protection Ombudsman and effort by the subject of the audit is also required. Great observations were made during the audits on how to develop the guidelines and training on the processing of personal data as a part of the accountability principle and in order to promote internal supervision of legality.

The audits did not indicate any need for the use of specific powers. The observations made in the audit reports have been taken seriously and the completion of corrective actions indicates that the competent authorities have understood the impact of developing data protection activities in contributing to both the legality of their actions and their effectiveness. The audits were particularly effective in developing the processing of personal data in connection to threat scenarios produced by the authorities.

Questions relating to the use of facial recognition technology remained a topical theme in the activities of security authorities. The police has extended its use of facial recognition technology to image materials captured in crime prevention, and during a prior consultation, the Office of the Data Protection Ombudsman helped to steer the activities of the police to ensure the methods used are legal. Valid legislation does not offer the opportunity of real-time online facial recognition in a flow of images.

The use of Clearview AI facial recognition technology was an additional cause of concern in Europe and quite legitimately so. In Finland, the issues related to said technology in the work of security authorities did not emerge until 2021, despite several supervisory measures, and the processing of this topic is ongoing while I am writing this. A relevant decision in Sweden is important in many respects. The controller remains responsible even if technology is used without consent – being aware of appropriate practices is the responsibility of the controller. A particularly conscientious approach is required to ensure and demonstrate the legality of measures when biometric data is involved.

In the development of legislation in the sector, automated decision-making continued to create controversy. The Act on processing personal data in immigration administration was adopted without provisions on automated decision-making primarily due to the lack of general administrative legislation in the field. The principles of personal data processing and the legislation concerning automated single decisions in particular can be similarly applied to the technology of automated decision-making in administration. The Ministry of Justice has drafted a memorandum and founded a committee to investigate legislative drafting of general legislation on automated decision-making in administrative matters. Hopefully, this work will proceed swiftly, and the development of automated decision-making in administration will proceed in a controlled manner.

“In 2020, the Office of the Data Protection Ombudsman conducted 11 audits of organisations of internal security.”

Despite the challenges presented due to the COVID-19 pandemic, most of the scheduled audits were completed, even though some special arrangements were needed. The experiences gained from virtual audits were mostly positive and it is likely that they will continued after the special circumstances due to the pandemic have passed.

With positive experiences obtained, the Office of the Data Protection Ombudsman will continue to carry out audits of the internal security authorities in line with the new model.



Jari Råman

Deputy Data Protection Ombudsman

Focus areas of data protection activities

The Office of the Data Protection Ombudsman imposed administrative fines for the first time

In May 2020, the Sanctions Board of the Office of the Data Protection Ombudsman imposed first administrative fines for breaches of data protection legislation. The task of the Sanctions Board is to impose administrative fines in line with the GDPR to the controller or processor of personal data. The Sanctions Board is made up of the Data Protection Ombudsman and two Deputy Data Protection Ombudsmen. The Data Protection Ombudsman is the Chair of the Board.

Imposing administrative fines is one of the corrective powers of the Office of the Data Protection Ombudsman. Administrative fines can be imposed in addition to or in place of other corrective actions. A corrective action used must be efficient and proportionate. The maximum amount of the administrative fine is 4 per cent of the turnover of the company or 20 million euros. Administrative fines cannot be imposed on public organisations, such as the government or state-owned companies, municipalities and parishes.

In 2020, the Office of the Data Protection Ombudsman issued

- 40 orders to notify data subjects of a personal data breach
- 33 orders to ensure the compliance of personal data processing measures with the GDPR
- 36 reprimands for processing measures that violate the GDPR

In 2020, the Sanctions Board imposed administrative fines on a total of five companies for breaches of data protection laws

- An administrative fine of 100,000 euros was imposed on the Posti Group due to shortcomings in informing persons who had submitted notices of change of address. The company should have informed their customers in an explicit manner that when submitting a notice of change of address, they are entitled to not to consent to the processing of their personal data and disclosing it for direct marketing purposes. The breach concerned 161,000 people in 2019 alone.
- An administrative fine of 16,000 euros was imposed on Kymen Veski Ltd for the failure to complete an impact assessment on the processing of their employees' location data. The impact assessment should have been completed prior to the company's processing of location data which was collected by geographic location of the vehicles using vehicle on-board systems.
- An administrative fine of 12,500 euros was imposed on a company that collected employees' data in an excessive manner. The company had requested for employment information that was not required for the employment contract, including information on their health and family relationships.
- An administrative fine of 72,000 euros was imposed on Taksii Helsinki for several shortcomings in its processing of personal data. The company had not, inter alia, assessed the legality of personal data processing regarding its camera surveillance system or informed customers of voice recording in a manner set forth by the GDPR.
- An administrative fee of 7,000 euros was imposed on ACC Consulting Varsinais-Suomi for sending electronic direct marketing messages without prior consent and for non-compliance of the rights of a data subject. The company had not responded to or implemented the requests concerning the rights of data subjects, and it was not able to prove that it had processed personal data legally.

Appointment of the Expert Board

For the first time, the Finnish Government appointed an Expert Board by virtue of the Data Protection Act. The Expert Board, operating in connection with the Office of the Data Protection Ombudsman, is tasked with issuing statements on significant questions related to the application of legislation pertaining to processing of personal data at the request of the Data Protection Ombudsman. The term of the Expert Board began on 1 October 2020 and will end on 30 September 2023.

The Board consists of a Chair, a Vice Chair and three Members, all of whom have a personal deputy member. The members of the Board are experts independent of the Office of the Data Protection Ombudsman. The Board may also consult other experts if necessary.

The Expert Board will convene as and if needed when summoned by the Chair. The Board has no formal decision-making authority.

Expert Board

- Chair:
Riikka Koulu, Assistant Professor
- Deputy member of the Chair:
Tobias Bräutigam,
Adjunct Professor, Attorney
- Vice Chair:
Tanja Jaatinen,
Senior Ministerial Adviser
- Deputy member of the Vice Chair:
Sami Kivivasara,
Senior Ministerial Adviser, Head of Unit
- Member:
Riikka Rosendahl, Team Manager
- Personal deputy member:
Antti Poikola,
Master of Science in Technology
- Member:
Kimmo Rousku,
General Secretary, Senior Specialist
- Personal deputy member:
Leila Hanhela-Lappeteläinen,
Data Protection Manager,
Data Protection Officer
- Member:
Tommi Toivola, Manager
- Personal deputy member:
Eija Warma-Lehtinen,
Lawyer, Partner

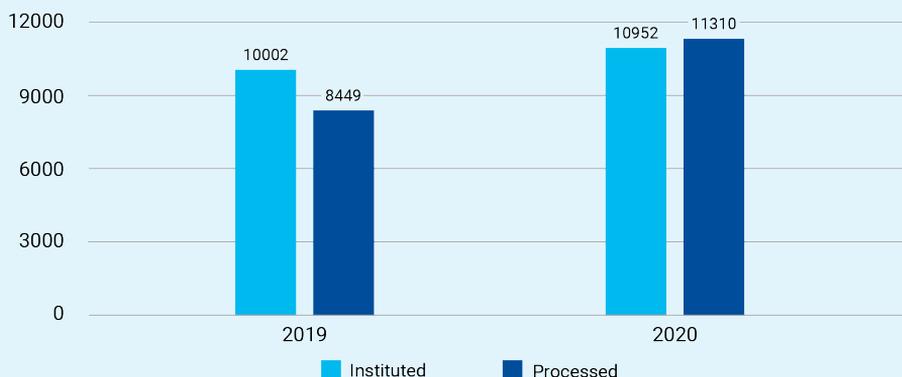
Measures to clear the backlog

In January 2020, the Office of the Data Protection Ombudsman launched a project to clear the backlog of unresolved cases instituted in 2014–2018. In early 2020, the number of these old, unresolved matters from 2014–2018 totalled 2,327.

In the end of 2020, the number of unresolved matters stood at a little over 400. Of these, 188 were cases that are processed in an international procedure and their processing depends on the actions of a supervisory authority of another country.

In addition to clearing the old cases, there were resolutions given for matters instituted in 2019 and 2020. In the end of 2020, the number of unresolved matters instituted from 2016 to 2019 totalled 1,550. The number of unresolved matters had been decreased by almost 800 from January 2020. The project of clearing the backlog continues at the Office of the Data Protection Ombudsman in 2021.

Matters instituted and processed from 2019 to 2020



Processing cross-border matters

Cross-border processing means either

- processing of personal data which takes place in establishments in more than one EU Member State where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in a single establishment of a controller or processor in the EU but which substantially affects 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. For cases that are processed in a cooperation procedure, a lead supervisory authority is appointed. Their task is to cooperate with the supervisory authorities that are cooperating in the processing. The goal of the consistency and cooperative mechanism is to ensure that the application of GDPR is harmonised across the EU member states.

The number started to increase for cross-border matters that were processed in a consistency and cooperative mechanism of supervisory authorities in 2020. In June, the European Data Protection Board (EDPB) published a [register](#) of decisions by supervisory authorities in a cross-border processing of matters.

In November 2020, the EDPB adopted its first final dispute resolution decision in a matter that was processed in a cross-border cooperation. The dispute resolution decision concerned a matter in which the Irish supervisory authority was acting as the lead supervisory authority and had issued a draft decision in a matter concerning Twitter International Company. The matter in question included a breach of data protection that affected

Of the cross-border matters that were instituted during 2020, the Office of the Data Protection Ombudsman was named as the lead supervisory authority in two matters and as a supervisory authority concerned in approximately 230 matters.

approximately 88,700 data subjects. Several concerned supervisory authorities gave their objections on the proposal for a decision by the Irish supervisory authority, after which the Irish supervisory authority transferred the matter to the dispute resolution mechanism of the EDPB. The Irish supervisory authority gave its final decision based on the decision of the Board.

The Office of the Data Protection Ombudsman, in cooperation with the Estonian supervisory authority, processed a matter in which a company organising dog trips in Estonia had updated a list on its homepage of people who owed money to the company. The company did not react when the Estonian supervisory authority first contacted it, but did remove the list after they were contacted again. The Estonian supervisory authority issued a notification to the company for a breach of data protection legislation.

Auditing activities

The Office of the Data Protection Ombudsman increased the effectiveness of systematic auditing activities of authorities of internal security during 2020. The Deputy Data Protection Ombudsman conducted a total of 11 audits of authorities of internal security during the year. Subjects of these audits included National Police Board, Finnish Security and Intelligence Service, Criminal Sanctions Agency and The Finnish Border Guard, Legal Register Centre and the Finnish Defence Forces.

The subjects of audits and the audited measures were prioritized on a basis of risk analysis and impacts. The objects reviewed have included instructions and training of personal data processing as a part of accountability and the practical realisation of internal legality control.

Various actions of personal data processing by authorities have also been audited, for example, the application of the Security Clearance Act and measures connected to risk assessments produced by authorities. Controllers have received many types of guidance as a result of the audits.



The number of personal data breaches continued to increase

Notifications of personal data breaches formed the largest individual group of matters instituted by the Office of the Data Protection Ombudsman. In 2020, a total of 4,276 notifications of personal data breaches were filed, with an increase of 437 from the previous year. If a personal data breach can cause risk to the rights and freedoms of natural persons, the Office of the Data Protection Ombudsman must be notified. The notification obligation started in May 2018.

The great majority of data breaches is due to working on several tasks at the same time and in a hurry. When personal data is processed, it is not a good idea to take up several things at the same time, because it increases the number of mistakes due to negligence. Data breaches can also be prevented by securing databases following the generally accepted practices, testing systems and by ensuring proper instructions.

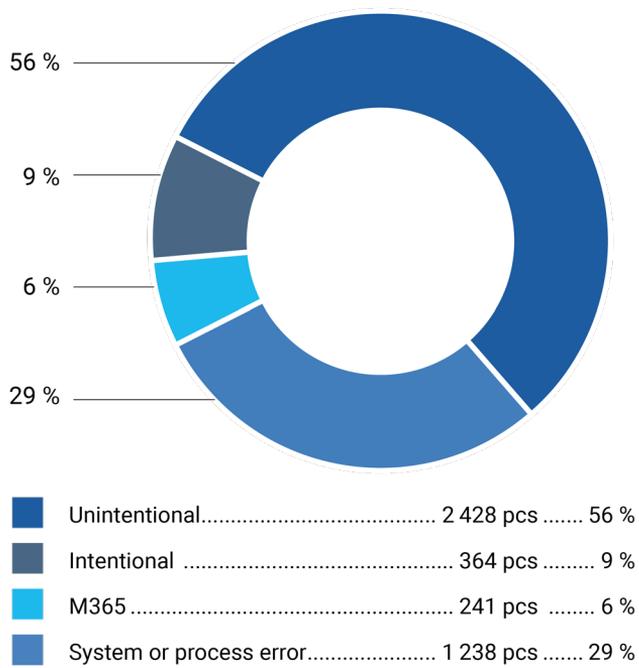
The single most significant data protection incident in 2020 was the security breach of Psychotherapy Centre Vastaamo, which became public in October. In this case, the personal and patient information of tens of thousands of people was stolen and leaked to the web. The Office of the Data Protection Ombudsman ordered that the company must inform all the clients affected by the breach personally.



The Office of the Data Protection Ombudsman was notified of 4,276 personal data breaches in 2020.

The Office of the Data Protection Ombudsman also initiated an investigation on the legality of the actions of Vastaamo. In the investigation, items reviewed will include the security of personal data processing activities by Vastaamo, informing of the data breach and the obligations of controller's accountability and whether following measures have been appropriate. The Office of the Data Protection Ombudsman coordinates the investigative measures in cooperation with the National Bureau of Investigation and other authorities. The intention is to complete the review even though the company was declared bankrupt in 2021.

Personal data breaches by type in 2020



Staff and finances

– new organizational structure established, changes in the assembly of ombudsmen

During 2020, the number of personnel in the Office of the Data Protection Ombudsman increased to 48 people. The recruitment process of a second Deputy Data Protection Ombudsman began in the autumn of 2020, after Deputy Data Protection Ombudsman Anu Talus was appointed the new Data Protection Ombudsman. Heljä-Tuulia Pihamaa, Master of Laws, was appointed to the post of Deputy Data Protection Ombudsman and started in the post in March 2021.

Three customer service teams are established in the Office; as a rule, one of them focuses on private sector and cross-border matters, the second on public sector and nationally processed 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. Administration, advisory and registry services are centralised in the Administrative Unit of the office. The Joint Functions team includes the IT

senior specialists, communications and the Data Protection Officer. The separate process groups also coordinate practices and projects on certain themes, such as data protection breaches, rights of data subjects and impact assessment.

In April 2020, the Office of the Data Protection Ombudsman relocated to new facilities in Lintulahti in Helsinki. Due to the orders and recommendations of virtual work as a consequence of the COVID-19 pandemic, the office introduced new kinds of digital working methods. In the new circumstances, the well-being of employees and occupational safety gained particular importance.

The project of clearing the backlog, which started at the beginning of the year, was apparent in the composition of the staff as new staff members were recruited. Four senior inspectors and two legal experts were working in the project to clear the congested situation

Human resources	2018	2019	2020
Number of personnel at the end of the year	31	46	48
Person years	27.4	40.6	45.6
Absences due to illness, day(s) per person years	11.5	11.5	10.7
Average age	42.5	41.6	39.9
Education index	5.7	6.3	6.3

Finances of the Office of the Data Protection Ombudsman	Realisation 2018	Realisation 2019	Goal 2020	Realisation 2020
Use of the operating expenses appropriation, €1,000	2,062	3,179	4,341	3,534
Total costs, €1,000	2,372	3,862	–	3,700

Matters instituted and processed from 2018 to 2020

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 2018–2020. The statistics have been retrieved from the document management system of the office for each 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 (groups 80–210).

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(3)) as well as issues related to lists of high or low risk processing measures.

	2018 Instituted	2018 Resolved	2019 Instituted	2019 Resolved	2020 Instituted	2020 Resolved
Tasks in accordance with the GDPR and the Data Protection Law Enforcement Directive (groups 80–210)	7133	3601	9292	7516	10233	10165
Prior consultation (high risk)	4	4	45	8	107	24
Statements	180	154	206	215	391	358
Codes of Conduct	3	2	1	1	3	0
Transfers of personal data	31	22	78	68	51	9
EU and international cooperation	647	217	1085	831	1091	825
Rights of the data subject	601	147	870	496	984	1085
Supervision	326	59	669	180	1009	943
Personal data breaches	2220	1100	3840	3620	4275	4139
Guidance and advice	1894	823	2014	1481	2081	2538
Data Protection Officers	1227	1073	483	616	241	244
Board of Experts	0	0	1	0	0	0
General issues (groups 01–29)	494	468	584	551	667	720
General, financial and human resource issues	404	368	580	545	667	717
Statements	78	89	1	2	0	1
Statements on administrative reforms	12	11	3	4	0	2
International matters (groups 30–39)	140	133	26	36	17	35
European Union	91	93	19	22	16	23
Other international cooperation with data protection authorities	12	11	6	7	0	2
Other issues	37	29	1	7	1	10
Ex ante control and guidance by the Data Protection Ombudsman (groups 40–49)	1632	2173	100	345	35	390
General guidance	166	185	87	100	33	33
Enquiries and requests for guidance by controllers	443	531	1	73	0	130
Processing of personal data with IT within the scope of the notification obligation	435	605	1	61	0	1
Statements to the Data Protection Board, Administrative Courts and the Supreme Administrative Court	5	5	0	0	0	0
Requests for information by the Data Protection Ombudsman	9	15	11	10	0	6
Enquiries and requests for measures submitted by data subjects	574	832	0	101	2	220
Orders of the Data Protection Ombudsman and other ex post control (groups 50–59)	212	335	0	0	0	0
Further methods related to inspections	1	3	0	0	0	0
Implementing the right of access of the data subject	78	97	0	0	0	0
Implementing a claim for rectification by the data subject	69	154	0	0	0	0
Statements to the prosecutor and courts of law	64	80	0	0	0	0
Applications to the Data Protection Board	0	1	0	0	0	0
Decisions of the Data Protection Board (groups 60–69)	0	1	0	0	0	0
Unclassified	6	5	0	1	0	0
Total	9617	6716	10002	8449	10952	11310



OFFICE OF
THE DATA PROTECTION OMBUDSMAN

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