OFFICE OF
THE DATA PROTECTION OMBUDSMAN

ANNUAL REPORT 2018

THE OFFICE OF THE DATA PROTECTION OMBUDSMAN

Data protection is a success factor

The Office of the Data Protection Ombudsman safeguards the rights and freedoms of individuals with regard to the processing of personal data. For us, data protection is a factor of success: for individuals, it means better protection of their personal data and the ability to manage it, while for businesses, it generates a competitive advantage based on responsible operations.

The Office of the Data Protection Ombudsman is an autonomous and independent authority that employs approximately 40 experts. The present Data Protection Ombudsman, Reijo Aarnio, has held the post since 1997. In the spring of 2019, the Office will see the appointment of two Deputy Data Protection Ombudsmen. The Data Protection Ombudsman and Deputy Ombudsmen are appointed by the government.

Our operating principles:
freedom of independent action, harnessing the power of the community, professionalism, proactiveness and guidance.

The cornerstones of our strategy:
anticipation and prioritisation, competence, guidance based on information and alliances.

Our values:
communality, fairness and independence, timeliness, creativity, transparency and intelligibility.

Our goals for 2017–2020

- 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.

Data Protection Ombudsman's annual review

The third page in the history of data protection was turned in the 31st operating year of the Office of the Data Protection Ombudsman, when the EU's General Data Protection Regulation (2016/679) was implemented on 25 May. At the same time, the Data Protection Directive (2016/680) updated the legislation on data protection in criminal matters. This directive also required national implementation measures (Act on data protection in criminal matters 1054/2018).

The GDPR also includes many directive-like features that require national implementation. Therefore, a national Data Protection Act (1050/2018) was drafted under the supervision of the Ministry of Justice and entered into force on 1 January 2019, replacing the previous Personal Data Act and the related Decree. The process also involved extensive amendments to national special legislation. The Data Protection Ombudsman was heard by Parliament 93 times in 2018. The work of the Parliamentary Constitutional Law Committee was particularly noteworthy. The Committee redefined its policies on enactments governing the protection of personal data and ruled that the GDPR essentially amounted to the level of data protection required by section 10 of the Constitution, also noting the risk-based approach of the GDPR.

New powers and duties

The GDPR entailed many changes. It significantly improved the rights of data subjects, imposed new obligations on controllers and facilitated operations in the digital single market. At the same time, it caused the upheaval of the century in the work and powers of the enforcement authorities.

One chapter in the history of data protection was closed with the dissolution of the independent Data Protection Board of Finland, which used to be the highest decision-making authority in the field of data protection. The work is continued by the European Data Protection Board (EDPB), which began operations in May. The EDPB and its various sub-committees launched their operations successfully, and an agenda was drawn up for the EDPB for 2019–2020. However, it seems likely that the capacity of the EDPB will be sorely tested by the growing number of cases in the near future.

The reform also gave birth to a new profession, the Data Protection Officer. The Office welcomes the new Officers and their assistance to data subjects and controllers as a positive development.

We were still forced to operate under two sets of legislation for part of the year, which naturally posed challenges to the service provision capacity of our Office. Another noteworthy feature of the past year was the explosive growth in case numbers. The Office of the Data Protection Ombudsman registered 9,617 cases instituted in 2018, while the corresponding number in the previous year was 3,957. The GDPR brought entirely categories of matters, such as Data Protection Officer notifications, notifications of personal data breaches and cross-border matters applying to several EU Member States.

Additional resources required

The Office of the Data Protection Ombudsman is seeking to adapt its operations to the data protection reform of the century by improving its competence management. We drew up descriptions of practically every new task appointed to the Office and updated our ERP system. Our staff did an unbelievable amount of work with the scant resources available. My heartfelt thanks to all colleagues for this.

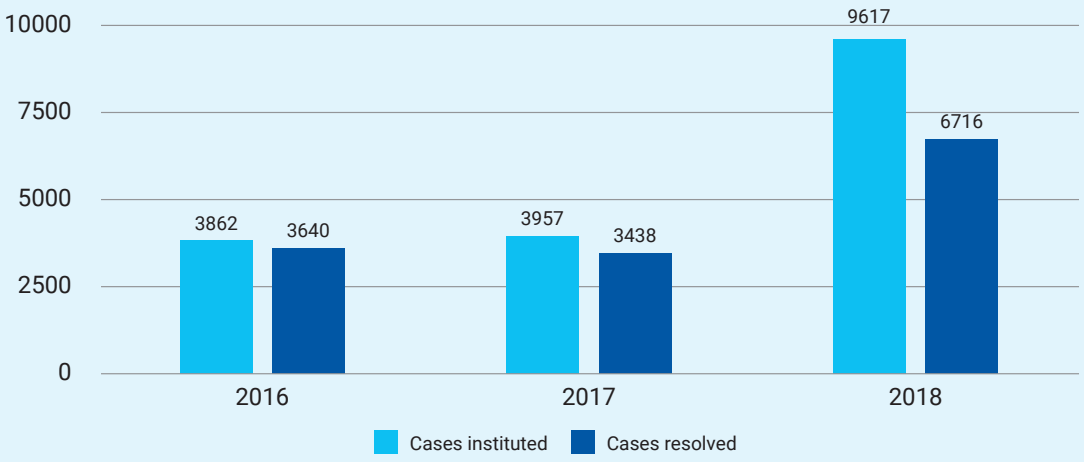
Thankfully, we were also assigned some extra resources. It is my belief that our competence in the subject matter is among the best in Europe! The recruitment process for two Deputy Data Protection Ombudsmen was started in late 2018. When they take up their posts, we will have the collegium required by the national Data Protection Act, enabling the Office to exercise the powers granted by the GDPR. The collegium is an internal body of the Office of the Data Protection Ombudsman with multiple members, which decides on administrative sanctions for infringements of data protection legislation.

The enactment of new intelligence legislation was also the subject of great interest in 2018. The Office was mainly involved with the oversight of legality in the process. After many and varied developments, the bill was finally passed this year. As a result, an independent Office of the Intelligence Ombudsman will be established parallel to the Office of the Data Protection Ombudsman.

Unprecedented interest in data protection

The Data Protection Ombudsman has witnessed some eventful years in the history of the office. In my experience, the past year was nevertheless completely exceptional in comparison to any that have gone before. On the one hand, the reform described above and, on the other, the Government's actions at the conclusion of its term made the year the most intensive in the memory of the Ombudsman. The media also expressed an exceptional interest in data protection.

Cases instituted and resolved

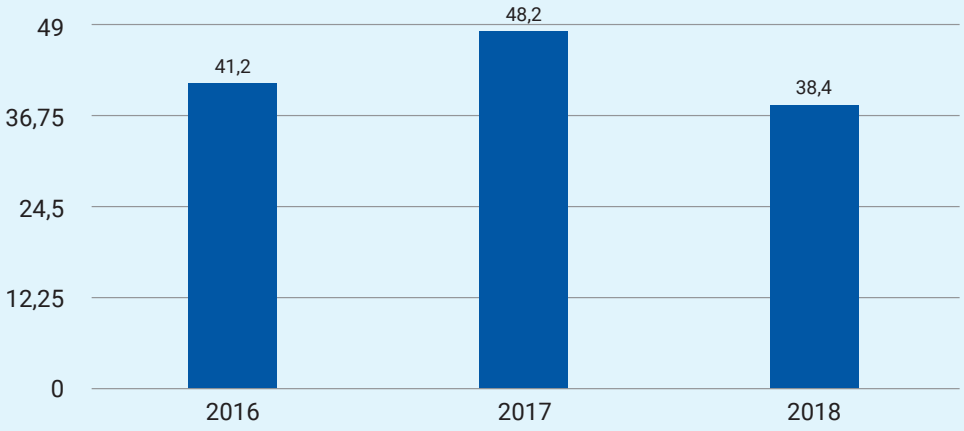


The entry of “top experts in data protection” to the market in such great numbers was also a new phenomenon, at least to myself. The early days of the GDPR were a goldmine for consultants. Unfortunately, the information offered to controllers was not always up to standard. These entrepreneurs ”marketed” the new legislation mainly from the perspective of sanctions. This had the effect of making some controllers turn in on themselves, while the purpose of the GDPR was to encourage businesses to seek growth on the digital single market by introducing common rules for a market of 510 million consumers.

Data protection is an enabler and a success factor. The approach of the 2019 elections revealed that it is also one of the safeguards of democracy. The Cambridge Analytica scandal was largely based on inappropriate profiling. In addition, our attention was drawn to the use of artificial intelligence. Digitalisation is proceeding, and providers want to make service provision faster and more cost-effective. The GDPR makes provision for approving the use of AI in national legislation, provided that appropriate measures are adopted for the protection of data subjects.

Reijo Aarnio
Data Protection Ombudsman

Processing time of the cases resolved (days)



Focus areas of data protection activities

As part of preparing for the implementation of the EU's General Data Protection Regulation, the Office of the Data Protection Ombudsman established process teams tasked with ensuring the uniform processing of cases in their area of responsibility and the development of processing.

Processing of personal data breaches launched

One of the most important tasks of the Personal Data Breaches process team is to ensure the smooth reception and uniform processing of personal data breach notifications. The process team consists of the Office of the Data Protection Ombudsman's legal experts and specialised IT experts specialising in personal data breaches.

The Personal Data Breaches process team helps the Office's other staff with the processing and evaluation of personal data breach notifications. To this end, the process team has drawn up internal guidelines for the assessment of risks and the processing of typical cases. In the case of atypical personal data breaches, the process team helps the referendary with the processing of the case.

The tasks of the Personal Data Breaches process team have been developed as needed. The team has drawn up new guidelines and modified the personal data breach notification form on the basis of feedback.

The obligation to report personal data breaches entered into force with the adoption of the GDPR on 25 May 2018. The Office of the Data Protection Ombudsman must be notified of personal data breaches if the breach could cause a risk to the rights and freedoms of natural persons.

The Office of the Data Protection Ombudsman was notified of 2,220 personal data breaches in 2018.

After notifying the Office of the Data Protection Ombudsman about the data breach, controllers can get advice relating to the protection of personal data and whether the people affected by the breach must be notified about the breach or not. If necessary, the Data Protection Ombudsman may order the organisation to comply with the obligations imposed by the GDPR.

Process team develops cooperation with Data Protection Officers

The Data Protection Officers process team supervises the reception and processing of Data Protection Officer notifications and improves the accessibility of Data Protection Officers and communications with them. In addition to legal experts employed by the Office of the Data Protection Ombudsman, the process team includes an information services secretary who maintains the register of Data Protection Officers.

Organisations have been required to notify the Office of the Data Protection Ombudsman of their Data Protection Officers since the entry into force of the GDPR on 25 May 2018. The Data Protection Officer is the organisation's internal data protection expert who monitors the processing of personal data and assists the management and personnel with compliance with data protection legislation. The Data Protection Officer serves as the contact person for data subjects and the Office of the Data Protection Ombudsman in matters concerning the organisation's processing of personal data.

The details of 1,227 Data Protection Officers had been communicated to the Office of the Data Protection Ombudsman by the end of 2018.

An organisation is required to appoint a Data Protection Officer if it

- processes sensitive data on a large scale;
- monitors individuals regularly, systematically and on a large scale; or
- is a public authority other than a court of law.

People are aware of their data protection rights

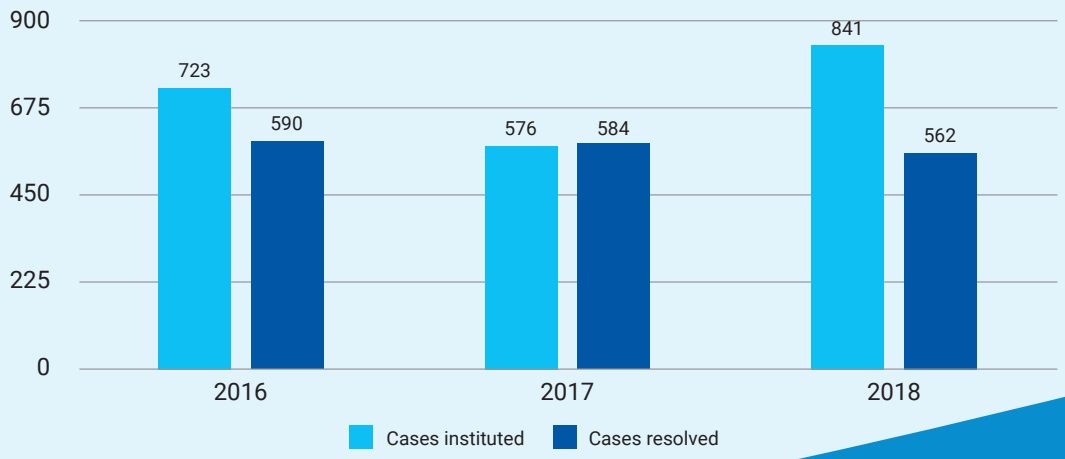
Matters involving complaints and the rights of the data subject are some of the most important aspects of the duties of the Office of the Data Protection Ombudsman. They include reports of the infringement of data protection rights and suspected cases of an individual or organisation processing personal data in violation of data protection regulations, but also various requests for advice or additional information.

After the implementation of the GDPR, the Office established a process team for matters involving the rights of the data subject, with tasks such as creating uniform procedures for processing complaints filed by data subjects. In its first year of operations, the team sought to prioritise matters with the most extensive or serious impact on data subjects and matters that had been in processing for a long time.

The cases instituted by data subjects are typically unique in their circumstances, which affects their processing and the time required for it. Complaints and legal questions in particular tend to require additional information, the acquisition and processing of which takes time.

You can expedite the processing of your case in the Office of the Data Protection Ombudsman by describing the matter as precisely as possible from the start. Assistance in this is available from the instructions and forms on the website of the Office of the Data Protection Ombudsman. The site also contains a service path for determining the best way to proceed with your case.

Cases involving the rights of the data subject



Impact assessments help identify risks

The impact assessment is a self-assessment tool provided by the GDPR to controllers for identifying threats to the rights and freedoms of individuals posed by the planned processing, assessing the severity and probability of the risks constituted by these threats, and adopting adequate security measures for dealing with elevated risks. Among other things, the impact assessment can be used to implement the data protection by design and by default and the demonstration obligation, referred to in Article 25 of the GDPR.

A prior consultation is required before the start of planned processing activities if the impact assessment indicates that the processing of personal data would cause a high risk to the rights and freedoms of the data subject and the controller is not able to decrease the level of risk through measures of its own. In the prior consultation, the controller contacts the Office of the Data Protection Ombudsman, which then issues written instructions for reducing the level of risk.

The impact assessment and prior consultation procedures were launched in 2018, with few actual procedures carried out yet. In the autumn of 2018, the European Data Protection Board confirmed EU-wide criteria specifying when an impact assessment is required. On the basis of these criteria, the Office of the Data Protection Ombudsman drew up the national list of processing types requiring impact assessments required by the GDPR. The list was published in December 2018 and covered the processing of data categories such as biometric, genetic and geographic data. The first prior consultations in Finland are expected in early 2019.

The new European Data Protection Board increased international cooperation

The European data protection authorities consolidated their cooperation further in 2018. The authorities prepared for the implementation of the EU's General Data Protection Regulation by drawing up guidelines and planning the activities of the European Data Protection Board.

The founding meeting of the EDPB convened on 25 May, the date of the GDPR's implementation. At the same time, the data protection authorities' cooperation body preceding the EDPB, the Article 29 Working Party, was dissolved. The Chairwoman of the Art. 29 WP, Andrea Jelinek, was appointed to continue as the chair of the European Data Protection Board. Jelinek's term will last for five years.

The European Data Protection Board is an independent EU body consisting of the Union's national data protection authorities and the representatives of the European Data Protection Supervisor. The EEA member states Iceland, Norway and Liechtenstein are also members of the EDPB by virtue of the EFTA Convention. The Commission has the right to participate in the activities of the EDPB and attend its meetings, but not to vote in them.

The European Data Protection Board is responsible for the uniform application of the EU's General Data Protection Regulation and the Data Protection Directive applying to police and criminal justice authorities. It issues clarifying guidelines and decisions on data protection legislation. A key task of the EDPB is to promote cooperation between the EU's data protection authorities.

In its first plenary session, the EDPB decided to support the guidelines drawn up by the Art. 29 WP on the application of the GDPR, and the preparation of the guidelines was subsequently continued by the EDPB. In the autumn, the EDPB published guidelines on, for example, the GDPR's geographical scope and certifications.

The first statements issued by the EDPB through the consistency mechanism were also finalised in September. The EDPB approved 22 statements applying to common requirements for data protection impact assessment lists. The statements were based on the national data protection authorities' lists of processing activities that are likely to cause a high risk and thus require a data protection impact assessment. Agreeing on common criteria is important to ensure the consistent application of the GDPR everywhere in the EU. The purpose of the GDPR was to harmonise data protection regulations, improve the protection of personal data and privacy rights, respond to new data protection questions related to digitalisation and globalisation, and to promote the development of the digital single market.

From the Office of the Data Protection Ombudsman, Data Protection Ombudsman Reijo Aarnio and Senior Adviser Anna Hänninen participated in the work of the Art. 29 WP and European Data Protection Board. Other staff also took part in the work of the sub-committees in their respective areas of expertise. In addition to the existing sub-committees, the Art. 29 WP established a new working group for data protection in the social media. The Office of the Data Protection Ombudsman is also represented in this working group.

The EU's General Data Protection Regulation contains detailed rules on cooperation between the supervisory authorities of EU Member States in cross-border matters. The general definition of a cross-border matter is that it has an impact on more than one EU Member State. The processing of such matters is conducted according to the one-stop-shop mechanism. This means that, in the future, controllers operating in more than one Member State can manage their cross-border matters through the supervisory authority of a single Member State. It is the task of this lead supervisory authority to coordinate the processing of the matter and draw up a proposal for a decision. The other supervisory authorities whom the matter concerns also participate in the handling of the case. EU authorities have a joint information exchange system, the IMI, for exchanging information on cross-border matters.

In the Office of the Data Protection Ombudsman, the coordination of cross-border and international matters was centralised with one senior adviser, supported by one adviser. They also take part in the work of the EDPB. In the spring of 2018, a process working group was also established for describing the processes related to cross-border matters.

Cross-border matters 2018

- Total: 591
- Finland as supervisory authority concerned: 106
- Finland as lead supervisory authority: 5

OFFICE OF
THE DATA PROTECTION OMBUDSMAN

P.O.Box 800, 00521 Helsinki, Finland
tel. +358 29 566 6700 (Switchboard)
tietosuoja@om.fi
www.tietosuoja.fi