Data breach targeting the City of Helsinki in 2024

P2024-01

FOREWORD

On 4 July 2024, the Government decided to launch an investigation into a data breach targeted at the City of Helsinki and set up an independent investigation team in connection with the Safety Investigation Authority. The decision to investigate the case is based on section 32 of the Safety Investigation Act (525/2011). This is an investigation of an exceptional event referred to in chapter 5 of the Safety Investigation Act.

Chief Safety Investigator, Associate professor, PhD. (Health manag.) Hanna Tiirinki was appointed as Head of the Investigation Team, and PhD (Econ.), D.Sc. (Econ. and Business Admin.), M.A. (Psych.) Petri Koistinen, M.Sc. (Admin) Ville-Petteri Pulkkinen, ICT Expert Kimmo Rousku, M.Sc. (Tech.) Petteri Järvinen, M.Sc. (Tech.) Tomi Lounema and BBA, MA Lilly Korpiola were appointed as its members.

Päivi Korpisaari, Professor of Communication Law, Master of Laws with court training, was appointed as Senior Specialist in Legislation.

The case is also under investigation by the National Bureau of Investigation.

An investigation of an exceptional event is conducted following the principles of a safety investigation. The purpose of a safety investigation is to improve public safety, and the investigation is not conducted to allocate legal liability.

A safety investigation examines the sequence, causes and consequences of events as well as the rescue operations undertaken and the actions of the authorities.

The investigation report describes the course of events, the factors leading to the event and its consequences as well as safety recommendations addressed to the appropriate authorities and other instances regarding measures that are necessary in order to promote general safety, prevent damage and improve the effectiveness of the operations of search and rescue and other authorities.

The investigation report was circulated for comments to the most important actors involved in the event. Their comments were taken into account when finalising the investigation report. A summary of the comments is provided at the end of the investigation report.

The graphics and illustrations used in the investigation report were produced by Sole Lätti/Tiedekuvitus. The source of these graphics is not noted separately in the report.

The investigation report was translated into Swedish and English by Lingsoft.

The investigation report was submitted to the Government on 17.6.2025, and it was published on the Safety Investigation Authority's website at *www.turvallisuustutkinta.fi/en/*.

Investigation ID: P2024-01
Investigation report 3/2025
ISBN: 978-951-836-678-5 (PDF)
ISSN: 2341 to 5991

TABLE OF CONTENTS

1 EVENTS

An extensive data breach targeting the City of Helsinki was detected on 30 April 2024. The data breach targeted the network of the Education Division (KASKO) and its servers. When the breach was detected, the City launched countermeasures and managed to stop the attack. The actual scale of the data breach could not initially be grasped due to the time it took to determine the targets of the breach.

The stages of the data breach and the steps taken to manage it are described in the following chapters. The information was collected by analysing various logs[1] after the event, but as not all necessary log data were available, having a complete situational awareness of the events was not possible.

1.1 Stages of the data breach

In the spring of 2024, an unknown attacker attempted to hack KASKO's intranet by searching for vulnerabilities and trying out different passwords. More than 300,000 contacts were registered between 29 February and 4 April 2024. An externally visible VPN router[2] was targeted. It, however, blocked the attempts.

Another attacker with a different IP address collected information on KASKO's network environment on 15 March 2024 and tried out passwords between 8 and 12 April 2024. The attacker attempted to hack the VPN router using two known vulnerabilities. At 20:14 on 14 April 2024, the attempts led to the crashing of this technically obsolete router that had not been updated, however without gaining access to the intranet. They nevertheless yielded more information on the VPN device and network technology, which the intruder was able to exploit later. Due to insufficient monitoring, KASKO's internal surveillance failed to detect the preparations for the breach.

While the second attacker may already have succeeded in logging in to the VPN router on 18 April 2024, the actual data breach started at 13:17 on 25 April 2024 when the attacker logged into KASKO's intranet with the username and password of a lower secondary school student they had found on the dark net[3].

After hacking it successfully, the attacker surveyed the internal network by scanning 34 network ports at a total of 9,945 intranet IP addresses over two hours. These actions triggered alerts in firewall logs at 13:40 and 13:59 on 25 April 2024. However, since the city did not have a firewall monitoring service, no-one paid attention to the alerts.

The attacker logged in to KASKO's server environment for the first time using a remote desktop connection at 15:07. Shortly after this, the anti-virus software maintained by DigiHelsinki issued a medium-severity alert, according to which 122 attempts in total had been made from a Windows server to log into nine other servers.

[1] In an IT environment, a log file contains log data automatically generated by a system, applications, or network concerning events, user actions, system errors, and security-related incidents for analysis, troubleshooting, and monitoring purposes.

[2] VPN (Virtual Private Network) is a technology that creates a secure tunnel through the public Internet. It enables remote users to connect to intranet servers securely.

[3] The dark net is Internet content that can only be accessed with a specific TOR browser. The criminal marketplaces on the dark net sell the services needed by criminals as well as usernames, passwords and credit card information.

DigiHelsinki's service provider opened a medium-level severity level ticket[4] concerning the alert at 17:22 on 25 April 2024. The ticket was directed to another service provider at 18:36, but due to an error in the ticketing system, it did not reach the service provider in question.

At 16:36 on 25 April 2024, the attacker continued login attempts to KASKO's server environment using a remote desktop connection and, between 17:24 and 18:40 on 25 April 2024, they gained access to the data in the Active Directory user directories of two different domains. In addition, the attacker gained access to a server that controlled virtual server environment containing KASKO's Windows servers.[5] The attacker also succeeded in hacking the server environment responsible for backing up KASKO's servers and files. The server takeover and subsequent copying of data were made possible by a theft of passwords belonging to administrators of the relevant domains.

After gaining the required credentials and access permissions to the servers, the attacker started copying KASKO's files found on the network drive. The first file transfer began at 2:54 on 26 April 2024, at which time the attacker copied 1.03 gigabytes[6] of data from KASKO's network drive. After this test transfer, the attacker started downloading network drive files using intranet servers. The file transfer from them started at 0:01 on 27 April 2024. In four transfers, approx. two terabytes of data were copied in total. The file transfer from the last server ended at 8:11 on 30 April 2024.

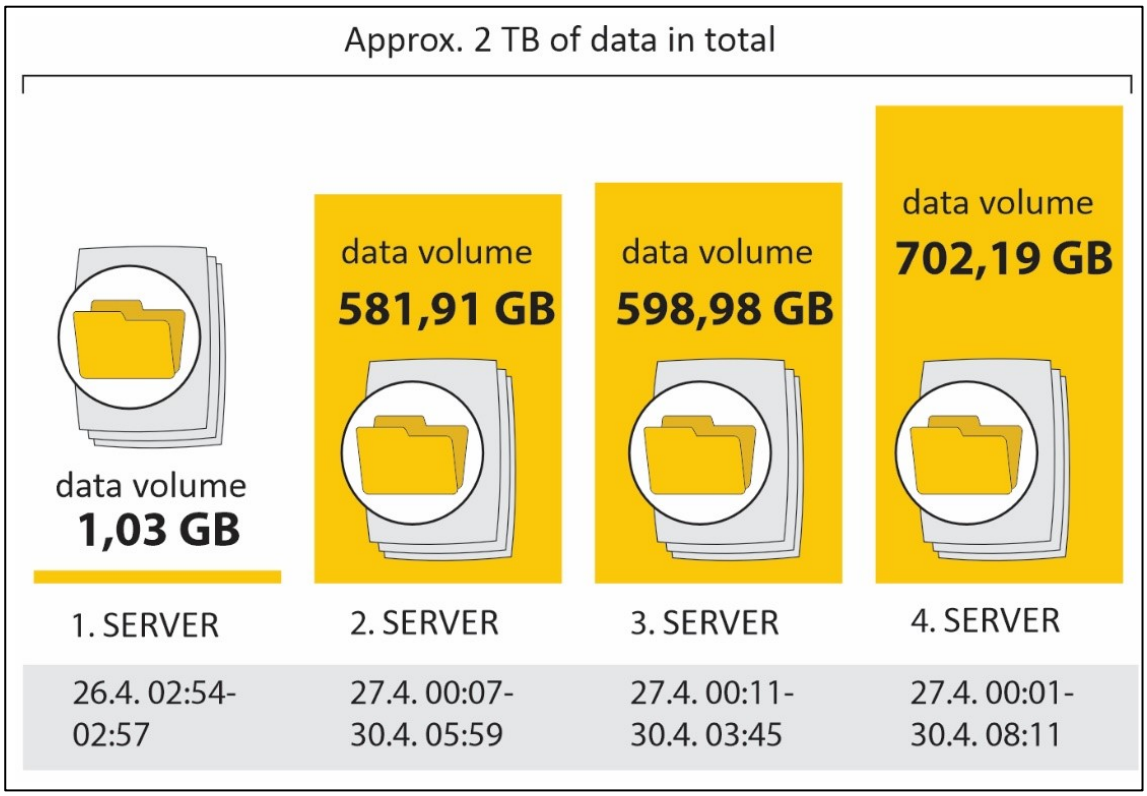

Figure 1. The attacker's file transfers in the data breach targeting the City of Helsinki.

[4] A ticket is a message in a specific format that indicates an observation or problem. The recipient takes action and closes the ticket when the matter has been resolved.

[5] A virtual server environment consists of a high-performance physical server environment which has a large amount of RAM and disk memory and which can run dozens or hundreds of virtual Windows or Linux server programs simultaneously.

[6] A gigabyte (GB) is a memory unit (one billion bytes). The memory can comprise internal random access memory (RAM) or permanent storage space (hard drives, USB flash drives, etc.). One terabyte is 1,024 GB.

Due to insufficient intranet surveillance and server logs, it was not possible to produce a complete list or determine the nature or number of the copied files. The attacker primarily copied data during the night at Finnish time, which reduced their risk of being caught.

DigiHelsinki's service provider only noticed the ticket left on hold at 11:34 on 29 April 2024 in one of the regular checks carried out at the time to identify integration problems. It was also found that the ticket's classification was medium importance, whereas the correct level would have been critical. The classification did not affect the delivery of the ticket, but it had been agreed that the delivery of a critical-level ticket would be confirmed by a telephone call.

KASKO's IT personnel were only informed of suspicious logins and attempts at breaking passwords detected on 25 April 2024 by an e-mail sent at 11:54 on 29 April 2024. An investigation was begun in KASKO, but it was slowed down by server modification work that was carried out at the same time. It was deemed possible that the alerts were irrelevant due to the server modification work.

On 29 April 2024, the attacker also tried to hack other Windows servers by breaking their passwords. At 01:30 on 30 April 2024, the attacker launched a brute force attack[7] to hack two more of the City of Helsinki's domains, targeting 165 network devices in total. At 03:10 during the same night, the attacker tried to access the networks of other City of Helsinki domains using the information they had collected.

Attempts to expand the attack by sending a query for administrator credentials to an AD server triggered a new alert with DigiHelsinki at night, at which time the service provider locked the credentials used by the attacker. The data breach began to be uncovered as a DigiHelsinki employee contacted a KASKO employee on Teams at 8:55 on 30 April 2024 to investigate the matter.

1.2 Detection of the data breach and actions taken

Information on the data breach detected during the night was conveyed to a KASKO cloud service team meeting at 9:30 on 30 April 2024. The investigation was then continued together with DigiHelsinki. The intruder had copied large number of documents from a server and the breach was hence a serious incident. KASKO decided to convene a meeting of the City level MIM (Major Incident Management[8]) group at 13:00 on the same day, after which MIM meetings were held regularly.

In the course of the morning, KASKO and DigiHelsinki experts located the attacker's entry route to the VPN device. Its connection to the City's information network was disconnected at 13:40 on 30 April 2024. The device's network cable was disconnected from the intranet in the data centre at 14:30. The device was left on, however, to preserve the data stored in its memory.

After losing access to KASKO's intranet, the attacker continued their login attempts for at least a week and possibly longer. The attempts failed, however, as their way in had been blocked by disconnecting the VPN router.

When traces of the data breach were investigated, unusual activity was also observed on the external backup server at 16:28 on 8 May 2024. The device was disconnected from the network, after which a scanner program found different versions of Neshta malware[9]

---

[7] A brute force attack means systematically trying out different password options until the correct one is found.

[8] The MIM group is an organisation's team responsible for managing major and critical incidents.

[9] Neshta is an old malware program, of which several versions exist. It collects information on the system and users that help the intruder.

frequently used in data breaches on its disk. The malware had damaged the operating system to the point where the server was no longer working and the backups were unusable. However, recovery and network cleanup could be carried out without backups.

KASKO launched remedial actions to implement a new backup service. Active technical management measures relating to the data breach were selected, and it was deemed that KASKO's information systems were secure in these respects.

The reports available to the investigation team showed that the attacker had attempted to hack a total of 1,700 computers in the City of Helsinki's network. They also included those in private schools in Helsinki, but the attempts had failed.

1.3 Data breach management

The City of Helsinki launched systematic data breach management measures at the first MIM group meeting held at 13:00 on 30 April 2024. The City and KASKO set up the following groups to command and manage the incident:

The **MIM group** met for the first time at 13:00 on 30 April 2024 and subsequently on a daily basis in May (32 meetings in total). From June on, the group continued to meet regularly several times a week.

The task of the **Education Division crisis group (KASKO MIM)** was to share and maintain situational awareness regarding the Division. The group met for the first time on 8 May 2024, and by 9 August 2024 it had held 15 meetings in total.

The City's coordination group decided on key measures related to managing the situation as well as communication issues on the presentation of the Chief Digital Officer, KASKO's divisional management and communications management. The group met 23 times between 6 May and 6 August 2024.

The task of the **preparatory group** was to maintain situational awareness, prepare matters for the management, and direct communication at City level. The group met for the first time on 4 May 2024, and subsequently almost daily until 31 May 2024, or 28 times in total. After this the group met nine more times prior to 10 July 2024.

The under the preparat group. It ensured that the targets and impacts of the data breach were assessed and the results of the assessment implemented. This included coordinating the City's **operative project group** was tasked to work and external actors' resources and coordination between the authorities. The group's tasks additionally included compiling situational awareness for the preparatory group. The group also prepared communication contents following the preparatory group's instructions and steered by the Communications. The group met for the first time on 6 May 2024 and eight times in total during May.

Responsibility for **communication** rested on the Communications Director on behalf of the City Executive Office and the Director of Communications and Marketing on behalf of KASKO. Together with the communication personnel, they formed a coordination group on enhanced communications. Among other things, interview requests by the media, updates of the FAQ page, dissemination of news, internal communication and the personnel's information security training were discussed in the group's meetings.

At the City level, the event was also discussed at the meetings of the communication, information security and data protection groups as well as in connection with the City Council's and City Board's meetings. The matter was also discussed in the Education Committee.

1.4 Communication of the data breach

The **City of Helsinki** provided information about the data breach on 30 April 2024 by publishing an incident banner on the City's intranet as soon as the breach had been detected and launched enhanced communication measures led by the City Executive Office. An *incident banner* was published on the City's intranet to provide information about the situation, and the Divisions' management teams were also kept up to date by email.

Iltalehti tabloid was the first to release news about the data breach at 20:31 on 1 May 2024 with the headline ”Suspicion: Russia-led security breach in the City of Helsinki's information network – Personal data compromised.”[10] The news spread widely in different media outlets.

The **City of Helsinki** published a *press release* at 13:25 on 2 May 2024 and reported on the data breach targeting the Education Division on its website.[11] In its press release, the City stated that the hacker had gained access to the usernames and email addresses of all City employees, as well as personal identity codes and address data of learners, guardians and personnel in the Education Division. This information was also passed on to the guardians of basic and secondary education students through the Wilma system and to day-care centres, which forwarded it to the parents. In addition, a news item about the event was published on the City's intranet.

As the task of communicating about a data breach and responsibility for providing additional information belong to the controller by law, in this case the City of Helsinki, the City Board and the committees, the City took the responsibility of coordinating communication. The victims of the data breach could not be identified individually, which is why the City told the Office of the Data Protection Ombudsman on 8 May 2024 that the data subjects would be informed by a public communication.[12]

On 7 May 2024, the **National Cyber Security Centre of Finland** set up an internal discussion group focusing on the data breach for the company investigating the data breach and key authorities. The purpose of the group was to coordinate the investigation and support communication.

The **City of Helsinki** next released information on the data breach at a press conference held on the *Helsinki channel*[13] on 13 May 2024. The representatives of the City of Helsinki, the National Cyber Security Centre and the police were present at the press conference. Five media representatives were present. An estimated 1,300 viewers watched the event live online, and the recording remained available for viewing on the City's website.

At the press conference, information was provided on the results of the data breach investigation, and victims were given instructions for protecting their personal data. The City of Helsinki stated that it will inform the data subjects by means of a public communication at *hel.fi/tietomurto* website. The website contained information on the progress of the investigation, answers to questions and instructions for data subjects.[14]

---

[10] Iltalehti news article 1 May 2024. 26/02/2025 https://www.iltalehti.fi/kotimaa/a/8d3e0f58-76fe-42e3-acb8-41f51eb70fac

[11] City of Helsinki: Public notice for possible target groups of Education Division data breach. 1 September 2024 https://www.hel.fi/en/decision-making/city-organisation/divisions/city-executive-office/education-division-data-breach/public-notice-for-possible-target-groups-of-education-division-data-breach

[12] Article 34(3)(c) GDPR.

[13] A channel which the City of Helsinki uses for live broadcasts and for publishing videos and podcasts.

[14] City of Helsinki: 1.9.2024 https://www.hel.fi/en/decision-making/data-breach

The police noted at the event that the injured party in this case was the City of Helsinki, and that there was no need for individual citizens to contact the police to submit their individual reports of an offence. The police also stated that they were investigating the case as aggravated unlawful access to an information system and promised to provide more information later.

Supervisors working in KASKO were informed by means of a Teams meeting. The City Manager sent out an email message to the City's personnel. Wilma system was used to inform guardians, learners and personnel in the City's basic and secondary education schools. In early childhood education, the message was emailed to families.

Helsinki Police Department announced at 14:26 on 13 May 2024 that they were investigating an extensive data breach targeting the City of Helsinki's network. The police are currently investigating the case as aggravated unlawful access to an information system.

The **Data Protection Ombudsman** communicated about the investigations of the data breach on 14 May 2024 and provided instructions for its victims.

The customers of the City of Helsinki's Education Division represent more than 100 different language groups.[15] Learners and their guardians were initially informed in Finnish, Swedish and English. Later more information was provided in such languages as Russian, Arabic and Somali.

A newsletter for the guardians of basic education students was sent out through the Wilma system, and a newsletter to guardians of children in early childhood education and care was sent out through the heads of day-care centres. Newsletters to learners at general upper secondary schools and Stadin AO Vocational College and their guardians were sent out using the Wilma.

Information on data breaches was added to Digipolku teachers' instructions. The City did not provide targeted and age-appropriate information for minor data subjects separately.

The City set up a helpline and a separate email address for guardians and learners. An electronic form was created for information requests, which went directly to the email address set up for the data breach.

The **police** reported on 17 May 2024 that the National Bureau of Investigation and Helsinki Police Department were investigating a case of aggravated unlawful access to an information system targeting the City's systems. The police instructed anyone suspecting that their personal data had been compromised to take measures to protect their identity. They said that the police are responsible for communicating about the criminal investigation, while the City of Helsinki as the controller informs residents of the data types that were leaked from the systems and the persons concerned.

The **City of Helsinki** published a *press release* on 21 May 2024 reporting on the progress made with the investigation and the fact that the potential target groups of the data breach were wider than initially believed. The release also noted that the hacker may have gained access to more extensive data concerning persons who have used the Education division's services than previously estimated. According to the estimate made at that time, the data breach concerned around 150,000 learners and their guardians. A similar message was sent out through the Wilma system for basic and secondary education, and the day care centres passed

[15] Vieraskielinen väestö: kieliperusteisen tilastoinnin ongelmia ja ratkaisuvaihtoehtoja (Foreign-language population: problems associated with language statistics and optional solutions). 15 January 2025 https://kaupunkitieto.hel.fi/fi/vieraskielinen-vaesto-kieliperusteisen-tilastoinnin-ongelmia-ja-ratkaisuvaihtoehtoja

on the message to guardians. The message was also sent to private day care centres as well as private and state-run schools. A message from the City Manager concerning the situation was sent to all supervisors of the City on Thursday, 23 May 2024. A message concerning communication about the data breach during the summer was sent out through the Wilma and the day care centres on 30 May 2024.

On 21 May 2024, the City of Helsinki published at *hel.fi/uutiset* a specialist's instructions on what action data subjects should take regarding the data breach and explained that the hacker may have gained access to data concerning all compulsory education age students in Helsinki. On the same day, the City announced in the social media service X that up-to-date information on the data breach can be found at hel.fi/tietomurto website.

Internal communication continued, and a letter to supervisors was emailed for information on 23 May 2024.

KASKO personnel were told that the surveillance of information security on the intranet had been stepped up.

Data subjects with a non-disclosure order could not be reached immediately after the data breach. An order of non-disclosure for personal safety reasons is an exceptional measure that restricts the disclosure of contact information from the Population Information System. The address and municipality of residence of a person with an order of non-disclosure may only be disclosed to authorities with permission to process data subject to a non-disclosure order.

As a later communication measure on 6 June 2024, the City published a news item relating that the Finnish Transport and Communications Agency had published instructions for protecting personal data in Somali, Arabic and Russian. On 18 June 2024, the City reported that the data breach against the City had not expanded further. A recording titled Turvaa yhteinen tietomme (Protect our common information) was published on the City's intranet on 7 June 2024.

An online news item reported on 8 July 2024 that more detailed information on the data breach had been provided to the Data Protection Ombudsman. On 12 July 2024, the City told the residents that an independent investigation group set up in connection with the Safety Investigation Authority, Finland would launch an investigation of the data breach targeting the City of Helsinki. Messages with similar content were sent out through the Wilma system for basic and secondary education, and the day care centres passed on the message to guardians.

Internal communication continued in June in form of intranet news and an update of the DigiABC training.

On 17 December 2024, the City published an online news item concerning the situation regarding the data breach and also passed on this message through the Wilma system for basic and secondary education. The message was also communicated to parents of children in early childhood education.

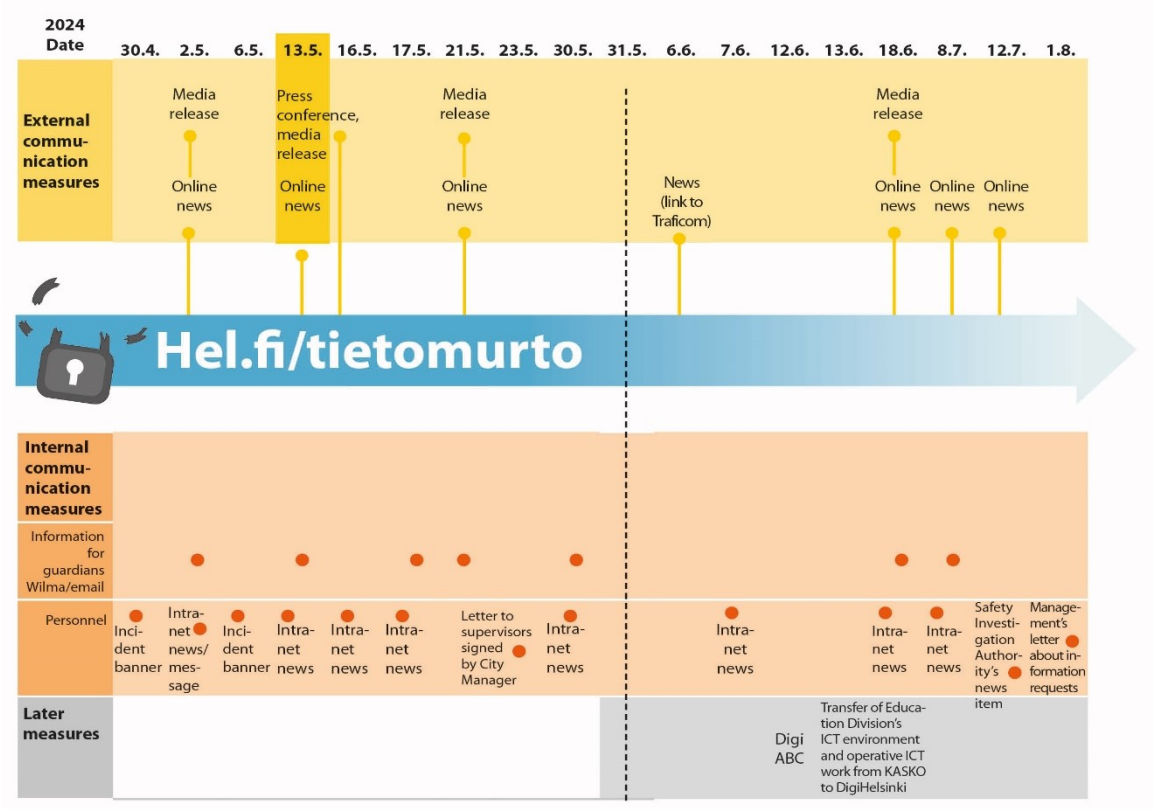

Figure 2: City of Helsinki's communication measures concerning the data breach.

1.5 Alerts and rescue operations

While the hacker attempted to operate as surreptitiously as possible by using the built-in commands and tools of the Windows operating system, the activity triggered alerts in the logs of both servers and network devices. Identifying the Living Off The Land (LOTL[16]) technique employed by the hacker was difficult as it relies on legitimate software and ordinary system components whose use does not usually trigger alerts.

Due to an error in the ticketing system, the alert of the malware protection software of 25 April 2024 did not reach KASKO. A notification thereof was further conveyed on 29 April 2024 - without receiving response. Only repeated alerts in the early morning of 30 April 2024 triggered a response at KASKO and DigiHelsinki.

[16] Living Off The Land is a cyber attack technique that, instead of malware, uses the target system's tools and resources for harmful purposes as far as possible.

Alerts in yellow

Date/time		Event	Attacker	City of Helsinki	KASKO	DigiHelsinki Oy	Commercial service providers	National Cyber Security Centre	Office of the Data Protection Ombudsman	Helsinki Police Department	National Bureau of Investigation	Finnish Security and Intelligence Service
2014		Cisco ASA 5515 VPN router purchased for Education service (KASKO's predecessor) to implement remote connections.			X							
2016		Last information security update of VPN router by KASKO, software from 2015.			X							
2017		Persons responsible for maintaining the VPN router leave KASKO.			X							
2018		A newer ASA 5545 is purchased in addition to ASA 5515 but not deployed before the employee responsible for the device leaves KASKO.			X							
2019		A contract award decision on purchasing new VPNs to replace old devices is adopted. No devices are purchased, however.		X	X							
2020		Transfer of VNP router users to DigiHelsinki's new remote use service begins.			X	X						
29.2.2024		Brute force attack on KASKO network 29 Feb–4 Apr 2024.	X									
31.3.2024		Using a remote connection, Dustin Oy updates the VPN router certificate. The certificate is valid for another year.			X	X	X					
8.4.2024		Brute force attack 8-12 Apr 2024 to gather technical information on KASKO's network and obsolete VPN router.	X									
14.4.2024	20:14	The attacker uses a known vulnerability and the VPN router crashes. The incident is not investigated in any detail.	X		X							
18.4.2024	11:17	The attacker probably logs in to the VPN router for the first time.	X									
23.4.2024	11:14	The attacker maps KASKO's IT infrastructure. This is recorded in logs but does not result in active monitoring or alerts.	X									
25.4.2024	13:17	The attacker gains a foothold in KASKO's intranet for the first time.	X									
	13:40	The logins trigger the first low-level information security alert at 13:40 and a higher-level alert at 13:59. Subsequently alerts from nine different devices.				X	X					
	15:07	The attacker's first login to KASKO's server via a remote desktop connection.	X									
	17:22	Anti-virus program gives alerts of failed login attempts. DigiHelsinki's sub-contractor opens a medium-severity ticket of their observations. At 18:36, the ticket is directed to another subcontractor who handles the integration of Helpdesk level 1 and other services for various suppliers.					X					
	18:40	The attacker has gained access to admin rights to two Microsoft Windows domains, the server controlling the virtual server environments and the backup system.	X									
26.4.2024	2:54	The attacker starts the first 1.03 GB file transfer to a server located abroad. The duration of the transfer is three minutes.	X									
27.4.2024	0:01	The attacker launches three larger file transfer to a server located abroad.	X									
29.4.2024	11:34	The alert (ticket) sent at 17:22 on 25 April is noticed and its processing starts. Due to a technical error, the alert had been left on hold.				X	X					
	11:54	KASKO receives the first alert of a potential data breach from DigiHelsinki's helpdesk service concerning login and password hacking attempts that took place on 25 April.			X	X	X					

Alerts in yellow

Date/time		Event	Attacker	City of Helsinki	KASKO	DigiHelsinki Oy	Commercial service providers	National Cyber Security Centre	Office of the Data Protection Ombudsman	Helsinki Police Department	National Bureau of Investigation	Finnish Security and Intelligence Service
30.4.2024	1:30	The attacker launches a brute force attack with 165 computers to access two other City of Helsinki Divisions. At 3:19, the attacker attempts to hack the intranets of other City of Helsinki Divisions, triggering alerts in anti-virus programs.	X									
	9:30	The alerts of the early morning are discussed at a regular meeting of DigiHelsinki and KASKO. The suspected data breach is confirmed, with dawning understanding of its seriousness.			X	X						
	13:00	Based on information received in the morning, the MIM group becomes operational and holds its first meeting at 13:00.		X	X	X						
	13:40	Investigations during the day confirm that the attacker has hacked KASKO's intranet through the Cisco ASA 5515 VPN router, which is disconnected.			X	X						
		The City of Helsinki notifies the National Cyber Security Centre, Office of the Data Protection Ombudsman and Helsinki Police Department.		X	X			X	X			
		The process of replacing critical network and server passwords is started.			X	X						
1.5.2024		Police report filed on 1 May in the morning.								X		
		Servers known to be hacked by the attacker are isolated from KASKO's network or shut down. The password replacement project continues.			X	X						
2.5.2024		Information exchanges between Traficom's National Cyber Security Centre and KASKO begin.			X			X				
3.5.2024		Commissioned by the City of Helsinki, an external service provider initiates digital forensics and incident response actions.			X		X					
		The hacked network drive is disconnected from KASKO's network and moved to another server whose security has been verified.			X	X						
		The Finnish Security and Intelligence Service contacts the City of Helsinki.			X							X
4.5.2024		The preparation group starts operating.		X	X	X						
		The external service provider launches 24/7 Security Operation Center (SoC) activities.			X		X					
8.5.2024		The backup system is found to be contaminated and useless, but it is not needed.			X	X						
9.5.2024		The National Cyber Security Centre starts special monitoring of the incident.			X		X	X		X		
13.5.2024		The City of Helsinki organises an open press conference.		X	X			X		X		
31.5.2024		The network drive is operative on a new platform and once again available for the personnel.		X	X							

Figure 3. Timeline of the progress of the data breach and recovery operation.

Actual IT countermeasures were launched at 13:40 on 30 April 2024 as KASKO and DigiHelsinki personnel prevented access to the VPN router. Experts first disabled the device and then physically disconnected it from the network. Power was not turned off, however, to ensure that the data in the device RAM[17] could be preserved for a closer inspection. To examine the log and other digital evidence found in the device, assistance of the manufacturer's expert services abroad were called upon.

At 17:15 on 30 April 2024, administrators of KASKO's internal network were prompted to change their passwords. Efforts to change the passwords for the local and technical usernames of servers were initiated at the same time and continued on 1 May 2024. On the

[17] RAM (Random-Access Memory) is the internal memory of an IT device.

same day, KASKO and DigiHelsinki began to isolate and shut down servers affected by the data breach.

Once the suspected data breach had been detected, the City of Helsinki notified it to the following authorities:

- The National Cyber Security Centre of the Finnish Transport and Communications Agency Traficom on 30 April 2024
- Office of the Data Protection Ombudsman on 30 April 2024
- A report of an offence was made to the police on 1 May 2024. It was recorded in the police systems as an aggravated unlawful access to an information system launched at 4:26 on 30 April.

At the time the notifications were made, the scale or severity of the data breach were not fully understood. The notifications described how the perpetrator had gained access to users' and administrators' usernames and email addresses.

The National Cyber Security Centre was first informed of the data breach targeting the City of Helsinki at 23:30 on 30 April 2024. The City of Helsinki submitted its initial notification using the “Report an information security incident” form found on the Cyber Security Centre's website. The first report was initially responded to within 12 hours of its submission, that is on 1 May 2024, by the Cyber Security Centre's duty officer. The Cyber Security Centre started information exchanges concerning this matter on the same day. Internal processing of the matter was initiated at the Cyber Security Centre at 19:30 on 1 May 2024.

The Cyber Security Centre assessed the severity of the incident on the basis of the information included in the initial report received by it. The assessment found that the case did not appear to require immediate action deviating from the Cyber Security Centre's normal processes. The reported information seemed to indicate that the City of Helsinki had the situation well under control: among other things, an external partner had been found to investigate the case, and restriction measures associated with the data breach had already been taken.

The Cyber Security Centre activated coordination of the data breach targeting the City of Helsinki between different authorities and other parties.

The Office of the Data Protection Ombudsman received the notification of the security incident and started processing it following its normal investigation procedure. The Office of the Data Protection Ombudsman did not take immediate action but asked for the material provided by KASKO to be supplemented. KASKO responded to the Data Protection Ombudsman's additional requests on 9 May 2024, 5 June 2024 and 8 July 2024.

The head investigator at Helsinki Police Department contacted KASKO on 2 May 2024.

On 30 April 2024, the City of Helsinki contacted a well-known commercial actor for assistance with managing and investigating the data breach, but the actor did not have the capabilities for delivering this service from Finland. KASKO then turned to Elisa Santa Monica, which started investigating the data breach at 8:00 on 3 May 2024. It set up a 24-hour Security Operation Center at 17:00 on 4 May 2024 and was able to initially verify that the hacker had only targeted KASKO's IT environment, without gaining access to those of the other Divisions.

Elisa Santa Monica concluded the data breach investigation on 11 September 2024 and submitted its report to the City of Helsinki on 7 October 2024. The cooperation continued with the provision of information security services to the City of Helsinki.

As a protection measure, geo-blocking was introduced on 2 May 2024, which prevented users located outside the Finnish borders from logging in to the City of Helsinki's services.

KASKO removed the network drive targeted by the hacker and prevented its use on 3 May 2024. At this time, the network drive was transferred from the server targeted by the data breach into a new, secure platform where experts were able to examine it.

The Finnish Security and Intelligence Service contacted the City of Helsinki on 3 May 2024 and requested additional information as a possible link to Russia had been brought up in the media.

The process of changing the passwords of server and network administrators and service IDs was initiated by administrators on 3 May 2024. In this connection, server authentication certificates were renewed and old certificates were disabled.

Technological and communication measures for managing the data breach

Elisa Santa Monica, which assisted in the investigation of the data breach, launched an examination (digital forensics and incident response service) aimed at identifying the scope of the hacker's access, preventing the spread of the attack to new devices and removing any active foothold of the hacker in the environment. The next key measure was ensuring that no back doors were left in the environment that would allow the hacker to regain access.

The company launched 24-hour Security Operation Center (SoC) activities, which were expanded on 14 May 2024 by installing more advanced terminal device monitoring sensors on KASKO's servers and devices to detect security breaches.

As a precaution, one domain controller server was shut down in two different AD domains to secure the data in the user directory.

New workstations guaranteed to be free from malware were deployed for administrators. Preparations for transferring files from the network drive targeted by the data breach to another server were initiated on 6 May 2024.

On 9 May 2024, work on capturing disk images of devices that were no longer connected to the network or under remote control began in order to determine the extent of the data breach.

As first response communication measures, the City of Helsinki immediately placed an *incident banner* on the intranet on 30 April 2025 and informed the public of the data breach on 2 May 2025.

The Finnish Transport and Communications Agency's Cyber Security Centre also assisted in the investigation, for example in the context of collecting data critical for investigating information security. It helped the City of Helsinki and the security service provider used by the City to gather forensic investigation data on the targeted servers that were critical for investigating the situation and scale of the data breach. The Cyber Security Centre also produced its own analysis of the event in the early days of the investigation as the situation was at its most serious.

Responses to requests for information

On 2 May 2024, the City of Helsinki started planning a service that could respond to access requests concerning personal data that had resided on the network drive. As no suitable off-the-shelf program was found, the Data and new technologies team in the City Executive Office's Digitalisation unit decided to build a separate system for this purpose.

On 13 May 2024, the City posted on its website an online form on which a strongly authenticated user could submit an access request concerning their and their dependants' data. The persons to whom this task was assigned then searched the documents for the details of the persons to be checked based on personal identity codes and student IDs. The results were sent to the data subject who had requested access either electronically by secure email or in a conventional letter, or they could be picked up at the Registry, as preferred by the data subject.

The search was limited to personal identity codes and student IDs, as distinguishing between persons with the same name is impossible when searching by name alone. It was also known that most of the documents containing personal data had one of these three unique identifiers. A free text search by name, address or phone number would have increased the risk of disclosing personal data to the wrong person.

The network drive that the data breach targeted was copied to another drive located in the data centre of DigiHelsinki's service provider on 19 May 2024.

The new network drive was technically operational and available to the personnel's use again on 31 May 2024 once its files had been scanned for any malware and their security had been ensured by means of two security programs. Users were instructed not to delete files or save new files to the network drive. They were told to save any potential new files to a personal H: drive.

1.6 Consequences

As a consequence of the data breach, a large amount of data from the AD user database and the network drive ended up in the hacker’s hands. They included personal data, some of which belonged to special categories of personal data[18] or were otherwise confidential.

The dataset targeted by the breach contained data concerning hundreds of thousands of people. Some of them were related to the personnel of KASKO or the City of Helsinki, others to students and their guardians. The network drive documents additionally included data concerning other persons, companies and other partners who had had direct or indirect dealings with the City.

[18] Special categories of personal data are data that reveal a person’s racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, sexual orientation or behaviour, or genetic and biometric data that can be used to identify the person.

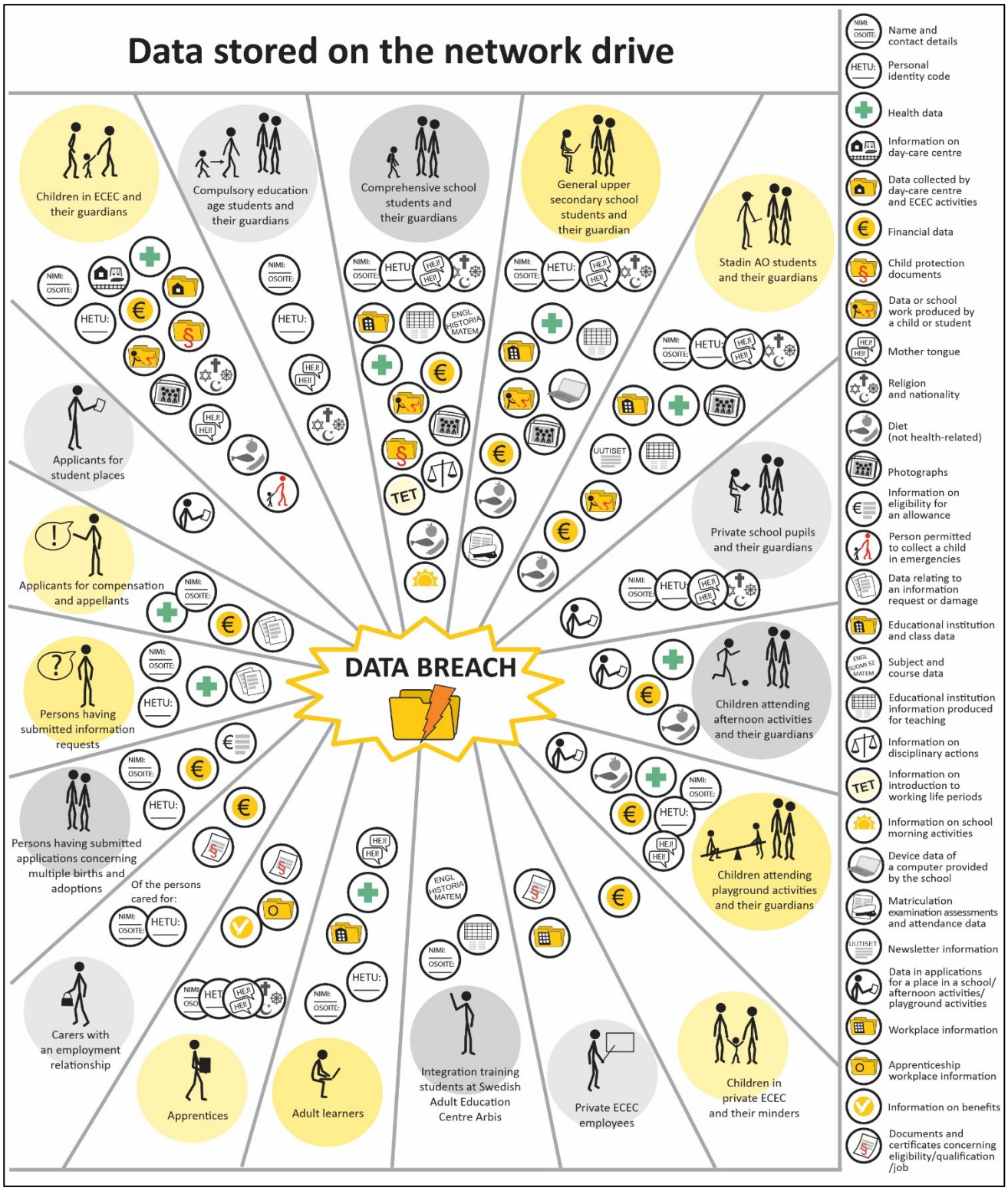

Figure 4. Data content stored on the network drive by group of persons.

The shutting down of the network drive hampered KASKO's daily work, especially in May 2024. Many information systems used for managing KASKO's IT infrastructure or providing services were unavailable, which had an impact on KASKO's internal activities and the functioning of the services offered to customers as late as autumn 2024.

The City of Helsinki incurred considerable costs from investigating the event and recovering from it. The immediate costs of investigating and recovering from the data breach in May–September 2024 were approx. EUR 650,000. In addition, the costs of commissioning new information security services amounted to at least EUR 400,000. Some of these investments can be included in the repair backlog arising from outdated IT infrastructure. The investigation of the event and the development measures launched on its basis also affect the implementation of planned ICT projects in other Divisions of the City of Helsinki.

The personnel of the City of Helsinki and its IT service subcontractors also had to do a significant amount of overtime, especially in May and June. These costs were not examined further as part of the investigation.

2 ENVIRONMENT, HARDWARE AND SYSTEMS

The City of Helsinki has almost 600 separate information systems. KASKO's own systems total around 300. This system configuration has evolved over a long period of time. The problems typical of such configurations are the fragmentation of systems, information exchanges between them and the management of their technical service life. The fact that standardised deployment procedures are not always used for information systems has also added to the difficulty of understand this configuration. Especially minor information systems intended for specific tasks only are commissioned and decommissioned as part of normal operational changes, and these changes are not always processed or documented.

The hacked network drive was not described in the enterprise architecture diagrams of the City of Helsinki's information systems. Apparently, the network drive was not included in the descriptions either because it was not regarded as an information system, or because network drives are becoming obsolete as various cloud service environments are introduced. Before the COVID-19 epidemic, the network drive played a greater role in the activities of the City of Helsinki's Education Division. Since then, Teams and Office 365 have been preferred as they are considered more agile than the network drive. This trend also continued after the network drive targeted in the data breach was reintroduced.

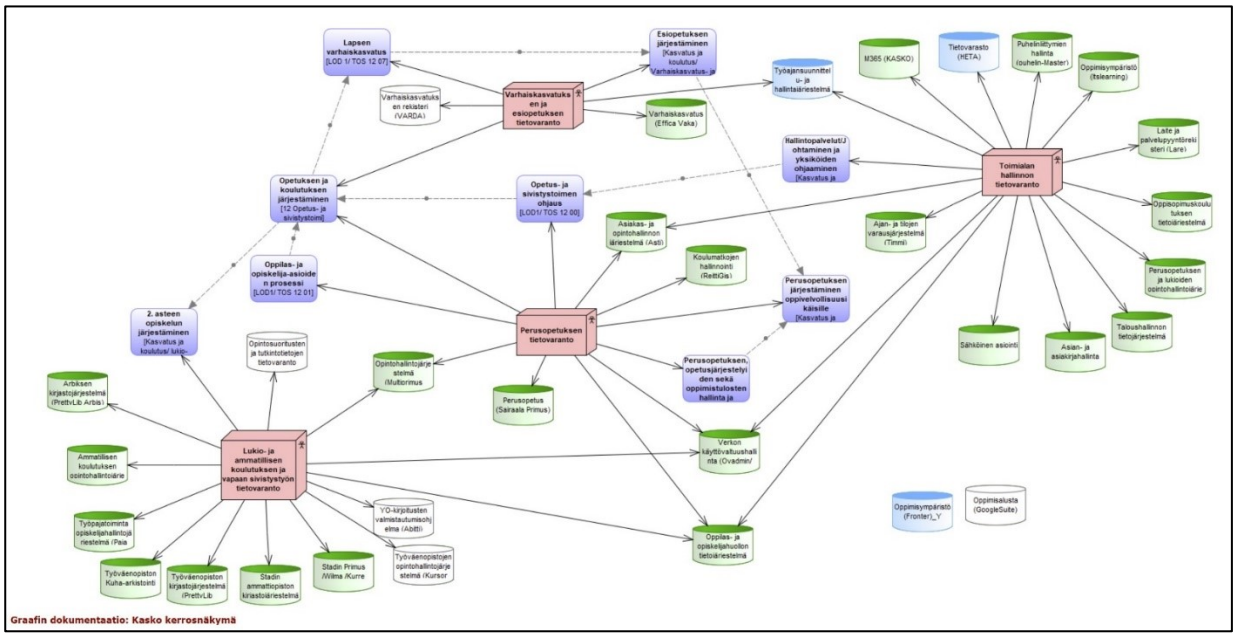

Figure 5. KASKO's enterprise architecture. (Figure: City of Helsinki)

The City of Helsinki has introduced M365 services offered by Microsoft gradually since 2022.[19] In connection with their deployment, the City has increasingly started using cloud services. Instructions for cloud service deployment in processing personal data had been issued by the City of Helsinki's City Manager on 12 October 2022.[20]

[19] Microsoftin M365-palvelujen käyttöönotto Helsingin kaupungilla (Deployment of Microsoft M365 services in the City of Helsinki). 26 February 2025 https://paatokset.hel.fi/fi/asia/hel-2022-012015

[20] Henkilötietojen ja salassa pidettävien tietojen maantieteellistä sijaintia ja siirtoa koskevat edellytykset (Preconditions for the geographical location and transfers of personal and secret data). 26 February 2025 https://paatokset.hel.fi/fi/asia/hel-2022-012014?paatos=252eaeba-1bed-4edb-a7a7-a0b55ee0f9f2

Ahjo[21] is the City of Helsinki's case management system. Responsibility for its development and system maintenance rests with the City Executive Office's Administration unit. Matters and documents initiated before the authorities are recorded and stored in Ahjo, and general administrative decisions, such as procurement matters, appointments to posts and matters related to financial decision-making are drawn up and saved in it. Official decisions related to special legislation or performing other special tasks are also handled in the City's other information systems.

The usual way of preparing a decision is that the person preparing the matter draws up a draft document and its attachments as Word or Excel files. The presenting officer stores these files on a network drive that is in their personal use, a cloud service or a shared network drive while the work is in progress. Based on these documents, a decision is prepared in the case management system by attaching documents, or copying texts from them to the decision document.

The problem with this workflow is that documents relating to a matter to be decided are copied to several storage locations, while only the actual case management system has features for managing the lifecycle of the matter. In other storage locations, document lifecycle management depends on user actions, such as deleting the file. The officers preparing administrative matters have been in the habit of keeping previous documents on the network drive and in the cloud service for later use as templates for preparing other matters.

According to the City of Helsinki's information management plan, some decisions have been made outside the case management system, and the documents of these decisions have been stored on the network drive. This applies to decisions concerning employer activities, in particular.

However, most of the documents to be prepared are typically other than actual decision documents. This is commonplace in de facto administrative activities, such as teaching. There has been no systematic management and storage environment for documents prepared for such purposes, and the practices followed have varied between authors and operating units, such as schools or day-care centres.

The City of Helsinki made a decision to procure a document management system on 8 November 2023. The decision could not be put to practice as the Market Court repealed the procurement contract on 26 April 2024 due to a formal error.

The **key customer information systems of KASKO** are Effica Vaka for early childhood education and care, MultiPrimus for basic education, general upper secondary schools and vocational education and training, AURA for student welfare in basic education and general upper secondary schools, AMMAURA for student welfare in vocational education and training, and Wilma for information exchanges between the home and the school. While the data breach did not target the datasets of customer information systems directly, it did target files that included reports on data in the customer information systems, or preparation documents to be stored in the customer information system. AURA and AMMAURA have since been replaced with Apotti, which is compatible with Kanta database.

[21] Ahjo is a document management system that can be used to send documents to right actors in the organisation.

2.1 VPN router data breach

The data breach targeted a Cisco firewall device of type ASA 5515 (Adaptive Security Appliance). KASKO used it as a receiving router for VPN connections.[22] A remote connection between a user's computer and the router is established using Cisco AnyConnect software, which provides the remote user with secure access to the intranet.

Figure 6. The hacked Cisco ASA 5515 VPN router photographed during the investigation in October 2024.

ASA 5515 is an inexpensive device with limited performance and features in Cisco's product range that supports at most 250 simultaneous users. It had been purchased for the use of the Education service, KASKO's predecessor, in 2014 to give the agency's IT personnel access to the education sector's intranet and also to the administrative network through a jump server. While the networks are fully independent, the jump server connects to both networks and enables controlled traffic between them.

Cisco's ASA 5515 model reached the end of its lifecycle in 2017 as product support for it was discontinued. In February 2017, the manufacturer announced an EOL (End-of-Life) schedule, according to which no more orders would be accepted after August of that year, whereas the availability of spare parts to customers with service contracts was guaranteed until August 2022. Software support continues, however, as the same software also works on more recent ASA series devices. At the end of April 2024, the latest software version was 9.12.4, which

[22] A VPN router is a device used by remote users to set up an encrypted connection through the Internet. The VPN (Virtual Private Network) then creates a protected tunnel through which the user has secure access to files and servers on the intranet.

should have been updated to the device to keep it as secure as possible. While a paid-up support contract is required for software upgrades, Cisco releases critical bug fixes for all users of the device.

KASKO was aware of the fact that support for ASA 5515 had been discontinued and, in late 2018, a newer ASA 5545 device was purchased for VPN use with the idea of duplicating remote access connections. However, the person responsible for purchasing and maintaining the device left KASKO in spring 2020 before the 5545 deployment had been completed. The preconfigured firewall device remained physically in the data centre rack above the old 5515 device, but it had not been connected to the network or mains supply.

KASKO's in-house IT personnel were responsible for the installation and day-to-day maintenance of ASA 5515. However, the key persons responsible for the device's information security left KASKO in 2017 without leaving any written documentation behind. In spring 2024, ASA 5515 was still in use without anyone to specifically monitor its operation.

In 2019, a proposal to procure two new VPN devices to replace Cisco's device was made. The proposal was adopted following KASKO's normal practices, but for unknown reasons these devices were never ordered.

Figure 7. Hardware cabinet at KASKO's data centre in October 2024. The image shows the backup VPN device ASA 5545, which was never commissioned. ASA 5515, which was used in the data breach, was located below it.

A **VPN router migration project** was launched in 2020, as the process of transferring KASKO employees' usernames from ASA 5515 to a newer VPN system maintained by DigiHelsinki began. The transfer project progressed normally but was not considered particularly urgent. Setting up schools' data connections and updating active network devices already created a heavy workload for KASKO's IT personnel.

In spring 2024, 20–30 usernames were yet to be migrated from ASA 5515 VPN device. Some users had credentials for both the new and old VPNs. The remaining users of ASA 5515 were mainly partner companies, such as employees of subcontractors responsible for surveillance cameras and access control equipment.

In 2019, the City of Helsinki was preparing its Digitaalinen perusta (Digital Foundation) project, which was launched at the beginning of 2021. The new organisation recruited two data communication experts from KASKO. At that time, the responsibility for providing data communications services was transferred to Digitaalinen perusta.

No written list was drawn up of the devices transferred from KASKO, which is why the status of ASA 5515 remained unclear. Digitaalinen perusta (incorporated as DigiHelsinki Oy at the beginning of 2023) felt that KASKO was still responsible for it. On the other hand, the practical maintenance work of ASA 5515 was also carried out by former KASKO employees who had transferred to DigiHelsinki's organisation.

The maintenance mainly consisted of updating the certificate and managing user IDs. As the edu.hel.fi certificate associated with the server's IP address is only valid for one year at a time, the certificate file had to be renewed regularly. DigiHelsinki commissioned this work from an external company with which it had an existing contract. The latest certificate update took place in March 2024 as the certificate was about to expire on 1 April 2024.

On Cisco's ASA devices, software and certificate updates can be carried out locally using a USB flash drive or remotely over the network. The commercial subcontractor company performed the requested maintenance actions remotely and tested them to check that they worked but did not check the software versions and operating settings of the server as a whole.

VPN user IDs for ASA 5515 had only been created for KASKO personnel members and the staff of outsourced service providers. Students did not have remote access credentials for the device. The VPN authenticated users based on a username and password. Strong authentication, such as one-time passwords sent as an SMS or a separate authentication application were not used because this could not be required of those who used their personal phones.

Principals, vice principals, special needs teachers and vocational education teachers had telephones purchased by the City, but only some of the other teachers had a phone provided by the employer. Personal phone users did not wish to install a separate authentication application on their phones or give their personal phone numbers to the employer, which is why strong authentication could not be implemented.

The **VPN router configuration** had an error that was critical in terms of the data breach. Typically, the configuration file contains dozens or even hundreds of settings that can be changed by using a graphical user interface or by editing a text file directly.

In addition to the technical operating settings, the configuration file lists the granted permissions to the internal network by user group. Unless a username belongs to one of the specified groups, it will receive default group-policy permissions. The VPN server configuration file had an erroneous setting:

```
default-group-policy AC-TUKI
```

This definition granted AC-TUKI group permissions to all those who did not belong to any designated group. The group name AC-TUKI refers to a group created by the IT support for itself in AnyConnect software, for which extensive access to all areas of the intranet was defined elsewhere in the configuration for troubleshooting and repairs.

The correct setting would have been:

```
default-group-policy DENY
```

This would have kept out users other than those specifically entitled to access the internal network. In the 5545 model purchased as a backup device, the DENY setting was correct.

The investigation was unable to determine why or when the incorrect settings were made in the configuration file. The original installers of the device had left the City of Helsinki's service in connection with an organisation reform in 2017. No previous versions of the configuration file were found from which the date of the addition could have been inferred.

The hacker managed to log in to the VPN router using the IDs and passwords of two students. It is likely that these data had ended up on the dark net as a result of a previous unspecified data leak.

Student IDs did not give permission to access the server remotely. However, the IDs matched the old user database of the education service, which is why the VPN router incorrectly granted them the AC-TUKI group permissions.

Technical access alone is not enough to read files or access file servers. This is why the hacker began to go through the intranet by systematically scanning servers and looking for ways to extend their access rights. By a method that the investigation could not fully detect, the hacker succeeded in using a remote desktop connection to log in to the intranet server with admin rights[23].

After gaining a foothold on the first intranet server, the hacker was able to hack other user accounts and consequently expand their access even further. What made things easier for the hacker was that the same password for the admin credentials was used on multiple servers. The hacker also gained access to the admin ID of the backup server, which allowed them to read the entire content of the file server.

On one of the servers, the hacker found the passwords saved to the browser's internal memory by an administrator. They included both personal passwords and passwords to KASKO servers.

2.2 Breach of the network drive

The Windows file server (later referred to as the 'network drive') was purchased for the education service around 15 to 20 years ago. The investigation was unable to learn the exact history of the device. Over the years, the number of users increased and disk space was expanded, which is why a large number of outdated files had been accumulated.

The hacked network drive could be accessed from all workstations and offices of KASKO administration, which meant it had several thousand users.

While the permissions to the network drive had been correctly divided between organisations and functions, this had no meaning during the data breach, as the attacker found a backup ID that had read access to all files.

There were differences in the way various offices used the network drive. Some hardly used it at all as they had deployed cloud services. In some units the network drives were used by all

[23] Admin (administrator) rights are more extensive than the permission granted to a basic user. With these rights, it is typically possible to change settings and manage other users' files. The admin rights can be device-specific or cover larger areas of the intranet (domain).

personnel members, in others by administrative personnel only. Different needs and established practices had resulted in differences between offices.

Most users saw the network drive as the V: drive of their computers. Some folders were shown as an R: drive. In addition to shared drives, users had personal network drives (H: drives) which were located in a different server environment and which the hacker had failed to hack.

The network drive is used to prepare, share and store data. The City of Helsinki has several information systems that are not fully interoperable. This is why it is necessary to keep documents in 'interim storage' on the network drive, making it possible for other users to edit them. Similarly, many decision documents are first drawn up on the network drive, and only the final information is recorded in the information systems in due course.

A great deal of different types of data had been saved to the network drive over the decades (see Figure 4). Some of the files were relevant to school activities, including instructions, newsletters and memos. Others contained confidential personal data, such as information about illnesses, allergies or medication.

Little was done over the years to assess or clean the contents of the network drive, and there were no clear instructions for using it. While general instructions for storing data on the network drive had been provided, compliance with the instructions was not controlled. Working documents intended to be temporary remained on the drive even after they were no longer used.

The network drive was a key tool for the units using it. Following the data breach, the network drive was out of service for about a month, which created a great deal of extra work for user organisations. The drive was out of service at the worst possible time, as certificates are drawn up in May, and pupil and student admissions for the following school year are prepared.

The network drive had been implemented as a virtual server located at KASKO's data centre. It was maintained by KASKO's in-house IT staff. There were plans to transfer the drive to DigiHelsinki's management by purchasing space in the subcontractor's data centre as a capacity service. However, the data breach took place before KASKO had time to complete the transfer.

Number and uses of files on the network drive

After the data breach, KASKO listed the files in the backup copy of the network drive. In its comments to the media, the City said that there were "tens of millions of documents on the network drive".[24]

The investigation team analysed the list of files on the network drive and found that it contained 4,983,854 rows in total. There were 521,774 folders and 4,462,080 files. The difference to the initially reported numbers is explained by the disk virus scan performed during backup.

The City of Helsinki released the total number of scanned files reported by the antivirus program. A virus scan opens all the file packages it finds, including ZIP files[25] as well as the CAB and MSI files[26] used for installing programs. Software distribution packages do not contain

[24] Yle news 25 May 2024: Helsingin kaupungin selvitys paljastaa yhä vakavampia piirteitä tietomurrosta (Investigation by the City of Helsinki reveals increasingly serious features of data breach). 26 February 2025 https://yle.fi/a/74-20090447

[25] ZIP is a commonly used lossless file compression technique that collates and compresses files to save disk capacity.

[26] CAB (Cabinet) and MSI (Microsoft Installer) are installation packages for Windows applications that contain all the files that the program needs and a digital signature of the program manufacturer that authenticates its origin.

user files, which is why they had no significance for the data breach. However, the virus scan also includes these files in the total number.

The operating system saves at least two timestamps for the files: the time the file was created and the last time the file was saved after editing. In some cases, the last time the file is accessed is also saved. This may relate to opening the file for reading or, for example, running a program file. The standard Windows file listing only displays the last time the files were saved.

As files from different sources had been collected on the drive over the years, the timestamps are not fully reliable in all cases. However, the stamps indicate that the largest number of new files was created on the drive in 2020 and 2021, after which the annual numbers of new files dropped by about one half.

Based on the edit dates, the highest number of files was modified in 2019, after which there also was a steady annual decrease in the number of edited files.

Key **documents saved on the network drive** include Word, Excel and PowerPoint files created in Microsoft Office as well as PDF files.

The investigation examined the file names on the list. They indicate that the Office documents included minutes, indoor air surveys, minutes of planning meetings related to renovations, sales receipts, layout and construction drawings, manuals, instructions, reports of offences, plans, annual reports and plans, and meeting agendas.

Table 1: Types and numbers of documents

Document type	Number
Word (DOC, DOCX)	1,094,684
Excel (XLS, XLSX)	513,060
PowerPoint (PPT, PPTX)	109,378
PDF files (PDF)	766,455
Total	**2,483,577**

PDF files can contain not only original documents but also scanned paper documents. Based on their names, the files included driving licences, hygiene passports, invoices, orders, medical certificates, applications for an assistant, press releases, personal fee calculations, leave of absence decisions, student assessments, tax cards, appointments to office, notices of resignation, accident reports to the insurance company and payslips.

Due to the nature of these documents, almost all of them presumably contain personal data that can be associated with and identify individuals. Particularly confidential documents included decisions on special support, information related to day care fees, medical certificates, passport copies and parents' personal and income data.

The volume of data can be illustrated by assuming that if printed out, each document would have five pages. This would mean a total of 12.5 million pages, and since one A4 sheet is approx. 0.1 millimetres thick, as a stack of one-sided A4 paper printouts they would rise to the height of 1.25 kilometres.

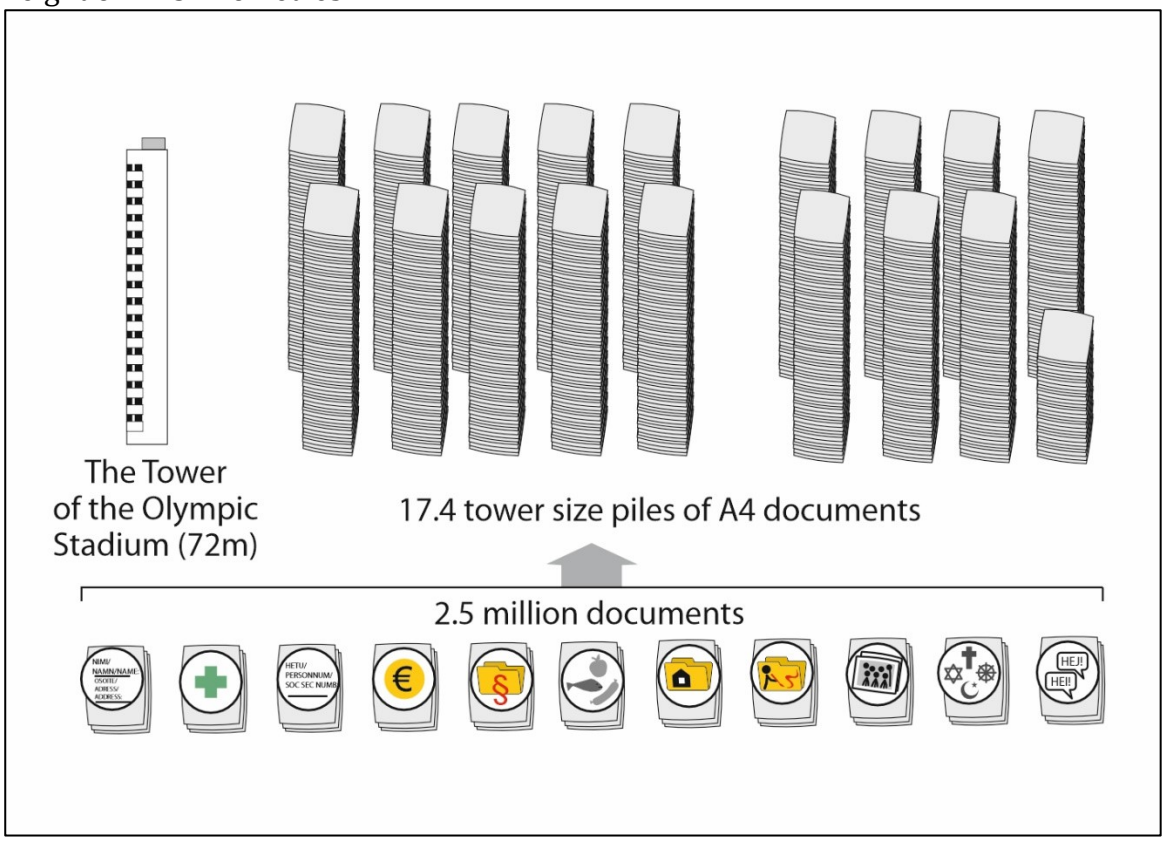

Figure 8. Illustration of the number of documents stored on the network drive.

Judging by folder names, the network drive also contained a large number of files transferred from other disks and backups made from USB flash drives. In addition to actual documents, there were more than 1.1 million JPEG images on the drive, including photos taken on day-care centres' and schools' excursions and at various events. Other file types identified on the network drive included video files, e-mail messages (MSG), web pages (HTM), animated images (GIF), ordinary text files (TXT), and software installation packages.

Due to inadequate log data, only an approximate idea of the **numbers of leaked files** can be formed. The files were downloaded to the attacker's server using a FileZilla's encrypted FTP[27]. The total volume of traffic could be determined from firewall logs, but due to encryption, file names or other details could not be established.

The attacker installed FileZilla on multiple servers but removed the programs after use, which is why the program logs did not help with the investigation. In one server's RAM, traces of transferred file names and network drive folders could be read, but the list was incomplete. It is consequently impossible to ascertain which individual files or folders the attacker gained access to.

[27] FTP (File Transfer Protocol) is an old method developed for file transfers. The original FTP transfers files without encryption, but the newer SFTP method (Secure FTP) used by FileZilla also includes encryption.

Based on the total data volume (two terabytes) the attacker downloaded in proportion to the total number of files on the network drive (6.73 terabytes), it can be estimated that 30% of the files were copied. In other words, the attacker gained access to around 1.3 million files, of which around 750,000 were documents (Office and PDF files).

2.3 Breach of user database

In addition to the network drive files, the attacker also hacked the user data in the City administration's AD database and the AD databases of basic education and vocational education and training. AD (Active Directory) is a centralized user directory of a Microsoft network that contains usernames and e-mail addresses together with personal data associated with them, and in KASKO's case, also student numbers.

2.4 Ability to monitor the network environment

Anti-malware software had been installed on the workstations in KASKO's intranet. Security software had also been installed on servers. However, KASKO did not have comprehensive surveillance capable of analysing network traffic and detecting anomalies.

The subcontractor who monitored the firewall services of KASKO and DigiHelsinki collects data on traffic between the City's intranet and the Internet. These logs have made it possible to retrospectively investigate events related to the preparation of the data breach and the actual attack between February and May 2024. The firewall services did not include real time alert monitoring.

The Living-Off-The-Land technique used by the hacker made it more difficult to detect the activity, as an active attack can mainly only be identified based on abnormal behaviour of the network and software.

From the hacker's 's perspective, the weakness of the method is not gaining a permanent foothold. If the criminal activity is detected, disconnecting, changing passwords and fixing vulnerabilities is enough to expel the hacker.

In an effort to improve the monitoring of the network environment, the City of Helsinki had launched the procurement of a Cyber Security Operations Center (CSOC) by publishing an EU contract notice on 28 June 2021. According to the contract notice, the CSOC would be procured to maintain the cyber security of ICT systems and services owned and managed by the City of Helsinki and those purchased or leased from a third party.

A response to the invitation to tender was received from one supplier. On 28 October 2021, the City Manager made a contract award decision on this purchase on the basis of the overall economic advantageousness, in other words the price, as the selection criterion. Minimum qualitative requirements (quality criteria) had been set for the services to be procured. The estimated value of the contract calculated over four years was EUR 5.2 million. The procurement contract was signed on 4 April 2022.

Once the contract award decision had been made, the supplier and the City started the commissioning project. As stated in the service contract, the commissioning project was concluded with testing the service. The City contracted an external operator to carry out the testing on 11 May–31 May 2023. The system failed the acceptance testing. DigiHelsinki issued a notice of termination to the supplier on 16 June 2023, and the commissioning project was interrupted.

2.5 Circumstances

In April 2023, the National Cyber Security Centre[28] and the Finnish Security and Intelligence Service[29] held a joint media conference[30], at which they noted that Finland's cyber security threat level had been first raised in collaboration with the two agencies in autumn 2022 and that it had remained elevated.

Reports received by the National Cyber Security Centre indicate that particularly the number of malware, phishing and denial-of-service attacks had increased among cyber attacks against Finnish organisations. According to the National Cyber Security Centre's analysis, attacks against Finnish organisations seemed more tailored and targeted. The Finnish Security and Intelligence Service confirms the National Cyber Security Centre's assessment regarding attempts at cyber espionage and cyber influencing.

A key factor raising the threat level has been the wider spread of cybercrime against both organisations and citizens. Government actors have also become active in the digital operating environment. In the 2020s, the spread of ransomware attacks has marked an essential change in information security threats against organisations. This phenomenon is discussed in the National Cyber Security Centre's review Information Security Now, which focused on Akira and Lockbit ransomware in September 2024.[31]

On 7 March 2024, or less than two months before the data breach, the Cyber Security Centre communicated about the risks of network edge devices and the way they open a door to an organisation's IT environment in its Information Security Now! article titled "Riskialttiit verkon reunalaitteet aktiivisten murtoyritysten kohteena"[32].

The Cyber Security Centre's monthly Cyber Weather[33] reports focus on significant information security incidents and phenomena in Finland. The Cyber Weather report on May 2024 was published on 13 June 2024. The introduction to the report notes that the Cyber Weather also remained cloudy in May. The situation was made bleaker especially by the data breaches and leaks that had come to light. The Cyber Weather summary table refers to the City of Helsinki case, noting that the City of Helsinki's Education Division had been targeted by an extensive data breach. The situation of data breaches in May was described as serious, which is the most critical assessment on the scale.

Most data breaches aim for financial gain. In some cases, the reason may be testing or showcasing the attacker's abilities, stealing commercially valuable data from a competitor, or exerting influence in society.

---

[28] Threat level in cyber environment has risen – activity towards Finland has increased 25 February 2025 https://www.traficom.fi/en/news/threat-level-cyber-environment-has-risen-activity-towards-finland-has-increased

[29] Threat level in cyber environment has risen – activity towards Finland has increased. 25 February 2025 https://www.traficom.fi/en/news/threat-level-cyber-environment-has-risen-activity-towards-finland-has-increased

[30] Cyber threat level remains elevated, targeted attacks have become more frequent. 25 February 2025 https://www.kyberturvallisuuskeskus.fi/en/news/cyber-threat-level-remains-elevated-targeted-attacks-have-become-more-frequent

[31] Akira- ja Lockbit-kiristyshaittaohjelmat valokeilassa (Akira and Lockbit ransomware in the spotlight). 26 February 2025 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/akira-ja-lockbit-kiristyshaittaohjelmat-valokeilassa

[32] Information Security Now! article "Riskialttiit verkon reunalaitteet aktiivisten murtoyritysten kohteena" (Risk-prone edge devices targeted by active hacking attempts) https://www.kyberturvallisuuskeskus.fi/fi/ajankoh-taista/riskialttiit-verkon-reunalaitteet-aktiivisten-murtoyritysten-kohteena

[33] Cyber Weather 26 February 2025 https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weath

2.6 Log data

The log management of KASKO's network devices, servers and terminal devices was mainly based on the devices' internal logs, for which there were no consistent practices or centralised management. This is why the data breach investigation had to partly rely on incomplete information. As key information sources emerged data from the firewall maintained by DigiHelsinki's subcontractor, which are mainly related to traffic between the Internet and KASKO's intranet. Little or no information was available on events affecting the servers and terminal devices of the intranet.

KASKO's service providers had certain server and network level surveillance services that triggered alerts of the hacker's 's actions in KASKO's server environment that were identified during the assessment of the data breach. The alerts were not monitored in a way that would have triggered preventive measures while the data breach was on going.

2.7 The City of Helsinki

The City of Helsinki is Finland's largest employer with approx. 37,000 employees at the end of 2023. The organisation has four divisions: Education (KASKO), Urban Environment (KYMP), Culture and Leisure (KUVA), as well as Social Welfare, Health Care and Rescue Services (SOTEPE). The City of Helsinki also has a central administration (City Executive Office). The Education Division targeted by the data breach is the largest of these four and employs around 15,000 people. The organisation of Helsinki is different from that of other Finnish cities in that the Divisions are highly independent and the role of the City Executive Office resembles that of a customer or supervisor.

The Education Division is responsible for early childhood education and care, pre-primary education, basic education, general upper secondary education, Finnish-language vocational education and training, and liberal adult education. The activities are highly extensive: for example, there are some one hundred comprehensive schools with around 45,000 students. The City has around 320 day-care centres, which provide early childhood education and care to approx. 27,000 children.

KASKO has its own administrative and support service organisation, which includes an information management function of around 80 employees. Of these, some 20 people work with ICT infrastructure and its information management. As a whole, information management has operated with a high level of independence and separately from the corresponding function in the other Divisions of the City.

The City of Helsinki adopted information security policies on 1 June 2020. These policies contained principle-level solutions binding on the City's organisation for promoting and ensuring information security. The document contains 14 different policies, including the grounds for the division of responsibilities.

The overall steering and coordination of the City's information management are carried out by an information management group appointed by the City Board on 21 March 2022. The task of the information management group is to coordinate the measures required for fulfilling the information management obligations at the City level, instructions, communication and training. The information management group develops, monitors, supervises and reports on the fulfilment of information management obligations in the City of Helsinki's organisation. The information management group's work has been regular and well resourced, and participation in it has been active. Through its work, the information management group has been

able to promote the fulfilment of the City's information management obligations and the development of information security. In the same spring, a dedicated information management coordination group was established in KASKO. It is tasked to coordinate the actions, instructions, communication and training required by information management obligations at Division level. The group's duties also include monitoring, supervising and reporting on the fulfilment of information management obligations in the Divisions.

The City's information management group prepares an annual information management supervision plan and discusses the situational reviews produced by the Divisions, unincorporated city enterprises and agencies. By means of the supervision plan, the City fulfils its statutory duty to control and supervise the processing of data.

The aim of self-monitoring is to develop City-level information management, address changes in practices and information systems, and report to the City Manager. The reports give a comprehensive picture of the work and observations of the information management group. The reports have also identified risks related to the information management environment, including the large number and fragmentation of information systems and inadequate information management environments.

An audit report completed by the City of Helsinki's internal audit function in February 2023 identified the fact that the sharing of responsibilities for information security between the City Executive Office and the Divisions (including KASKO) was unclear. A recommendation was issued, according to which KASKO should update its table of responsibilities by the end of September 2023. A survey was conducted as part of the audit, in which KASKO had the highest level of satisfaction with its level of information security of the four Divisions examined.

The report also identified that the City of Helsinki does not have effective means of detecting cyber attacks. Some of the reasons for this included delays in the procurement and commissioning of the service purchased for this purpose. A recommendation was made to obtain a centralised surveillance service by the end of May 2023. Due to the failure of the tendering process, the service could not be procured by May 2024, and it was consequently not in use as the data breach took place.

Office holders' responsibilities

By its decision of 28 February 2022, the Helsinki City Board adopted the City of Helsinki's guidelines, practices, responsibilities and control mechanisms for information and document management. According to this decision, the senior office holders of the Divisions, agencies and unincorporated enterprises are responsible for implementing information management measures. Senior office holders designate the parties responsible for their implementation in their organisations.

Responsibilities at the City level are laid down in the minutes of the City Board's decision referred to above. The Chief Digital Officer is responsible for City level steering related to the information management model and information management. In particular, the Chief Digital Officer is responsible for organising the planning, instructions and follow-up of implementation relating to the current state descriptions and change impacts of information systems and pools as well as to integrations and interfaces referred to in section 5 of the Act on Information Management in Public Administration[34] at the City level.

[34] 906/2019.

The Head of Information Management directs the City's document management, issues instructions on responsibilities, tasks and practices related to document management, guides and develops the City's document management as part of information management, approves the City's joint information management plan, supervises compliance with instructions, and takes care of training and advice provision associated with document management (including responsibility for directing information security related to the archivability of analogue documents, archive facilities and the protection of documents in exceptional circumstances).[35]

The organisation of development tasks in this thematic area in KASKO was similar to that of the joint development teams in the City's organisation. Four separate working groups had been set up for development tasks, and experts from the Division had been appointed as their members. The purpose of this was to ensure that the amended obligations under the Information Management Act and the General Data Protection Regulation can be met. As the working groups performed their duties, however, it turned out that there were too many groups and that their activities were poorly coordinated. For these reasons, the working group arrangements were later reformed.

On 28 May 2020, the Head of Education Division made a decision on the information management responsibilities of the office holders subordinate to them. The decision allocated tasks related to data protection, information security, information management and IT solutions to office holders in the sector. These tasks were described by characterising their contents in short sentences or keywords. Key office holders included the Administrative Director, Head of Information Systems and Head of Information Management, as well as the Head of Information Security who heads the unit, working in the capacity of an employer.

The City of Helsinki has extensive **instructions on information management, data protection and information security**. Some of them are shared by the City, while others are internal instructions of the Divisions. The Information Management Unit located in the City Executive Office has maintained 33 separate instructions on information management and information management practices.

On 27 September 2022, the Information Management Steering Group prepared a guide on official responsibilities for information management. The guide was aimed at the City's supervisors as a general presentation. The document described the structures for implementing information management. Among other things, it states that the City must keep a case register of the matters it processes. This includes matters in which some type of a decision is made. The officials preparing the matters must ensure that the processing stages of the matters and the relevant documents are registered without delay, keeping the register up to date. According to this guide, not all documents belong to the case register, as they are subject to the provisions on management of datasets in service production laid down in section 27 of the Information Management Act. Documents related to work duties must be registered and managed so that they can be found easily, even if no administrative decision has been made on them.

The guide also states that the information management model must contain an entry indicating the format, preservation method and retention period of the datasets and an indication of when the data should be destroyed if legislation or the information management plan so specifies. Permanently retained data must be stored appropriately, and data to be destroyed must be destroyed at the expiry of the retention period. The systems in which

[35] Delegation decision of the City of Helsinki (24 April 2017, section 441).

documents are produced for the case register must be described in the document publicity description.

The City Executive Office's guideline 'Temporary instructions on the electronic storage of data' dated 14 March 2022 states that documents must be drawn up and stored in the centralised document management system (Ahjo). However, the guideline allows such exceptions as the following:

> "*The City cannot as of yet offer digital tools for managing all tasks, which is why work is also carried out analogously, in other words using paper documents. A procurement of case management and document management solutions is being prepared. In the absence of city-wide preservation solutions, a temporary solution for digital preservation must be found, as the obligation entered into force on 1 January 2022. Documents for which there is no suitable digital information system are stored on a network drive in a shared folder*."

The **information management model** that directs the activities of the City of Helsinki consists of a number of different modules. It includes descriptions of information resources and information systems (architecture diagrams), application lists, process descriptions, information management plans and risk assessment documents. In addition, the information management model can be deemed to include the decisions on accountable persons and decisions-in-principle.

The architecture description of KASKO's information system presents the information systems used in the sector, its information pools and the general principles of information management. The network drive targeted in the data breach was not included in the descriptions.

The City of Helsinki maintains an **information management plan** as part of its information management system.[36] The idea is that the system would contain all information management data of the City of Helsinki, regardless of their format (digital and paper documents).

An information management plan that covers all task categories was completed in 2019. The plan is updated continuously, and an up-to-date version is available in the information network.

The employees have found KASKO's information management processes complicated. For example, they may need to print out an electronically signed form, sign it manually, and scan it into the system. In some schools, the network drive is only used by the principal and the school secretary. Teachers also use other solutions, such as existing cloud solutions and storage space on their personal computers. There are differences between schools and individuals in the procedures used for storing data.

DigiABC training for employees

The City of Helsinki has produced a video training course on data protection and information security titled DigiABC. Employees can complete this training, which takes about one hour, as self-study on their own computers. The training concludes with a multiple choice test. The City Executive Office has also produced teaching videos on information security for open viewing on the Internet.

---

[36] City of Helsinki: Tiedonohjausjärjestelmä (Information management system). 26 February 2025. https://tiedono-hjaus.hel.fi

As a basic premise, a new employee must complete the DigiABC training within two weeks, but the completion rates vary by sector. The content of the training videos is updated regularly, which is why those who have been KASKO employees for a longer period must retake the test. Supervisors monitor the number of training completions. The City has also offered basic courses in information and document management.

In spring 2024, the DigiABC training covered not only general information security issues but also data classification and security markings. General guidance on data protection was provided relating to the significance and secure processing of personal data. The life cycle of data and deletion of outdated data were not mentioned specifically.

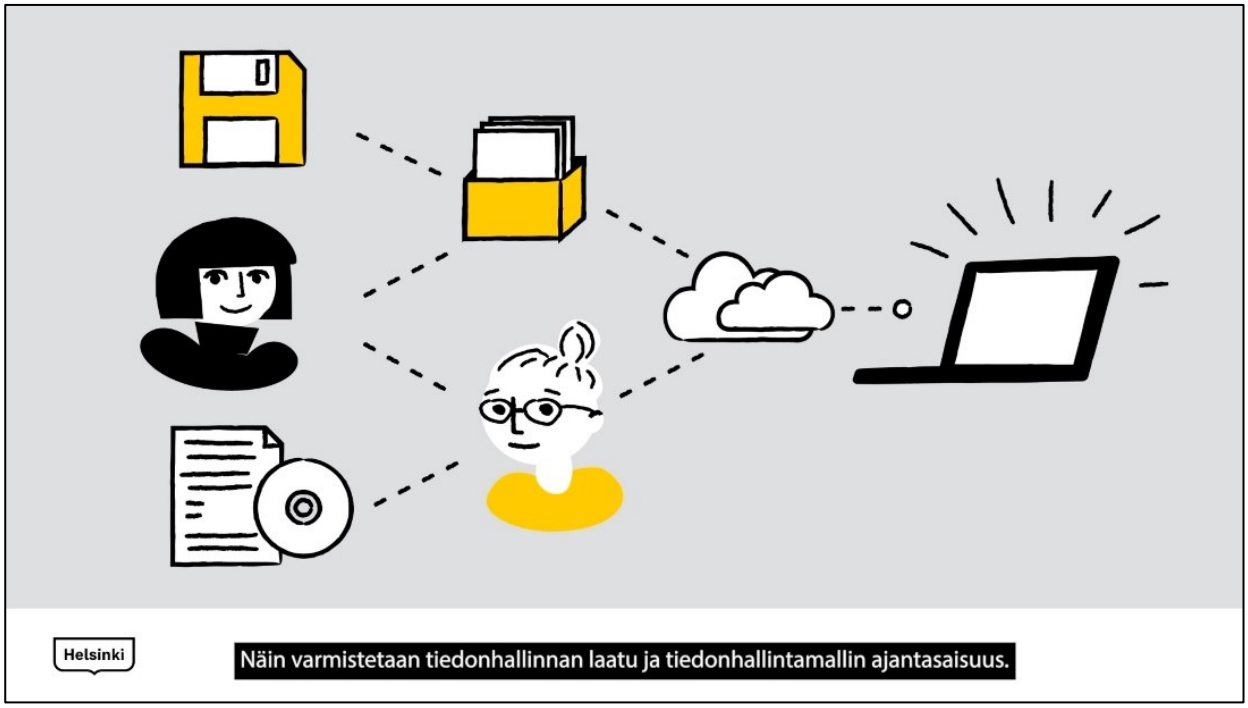

Figure 9. Screenshot of the City of Helsinki's DigiABC online training.

DigiHelsinki Oy, a limited liability company and part of the Helsinki City Group, was entered in the Trade Register on 2 August 2022. In 2023 its turnover was approximately EUR 58 million and it employed 134 people. The City of Helsinki fully owns the company's shares and exercises decisive control over the company's strategic objectives and important decisions as referred to in the Act on Public Procurement and Concession Contracts through its right to appoint Board members, ownership steering and group oversight.

The company's task is to provide basic digital services for the City of Helsinki. These services include the first level of support, support services for the meetings of elected officials' organisations, local support service, lifecycle services for terminal devices, standard software services, printing services, local area network, telecommunication interfaces, firewall, backbone network, server and storage system capacity services, database services, backup and recovery, AD directory, working group services, IT expert services, cyber security service, client workstation support services and information display service.[37]

The backdrop to the establishment of the company is the Digital Foundation project launched in 2019, the purpose of which was to initiate measures aiming to update and modernise the

[37] City Council, article 142, 1 June 2022

City’s digital operating environment. This project was included in the City of Helsinki’s wider digitalisation programme for 2019–2022 and was its key development target. The project was organised as part of the operations of the City Executive Office's strategic department, and some of the City’s IT staff moved to a unit established in the City Office. The activities continued in this form until early 2023, at which time these functions were transferred to DigiHelsinki Oy, a company established to provide the services. As a result of the incorporation, more of the City's IT staff members were transferred to DigiHelsinki.

Under the incorporation decision, DigiHelsinki Oy operates as the central purchasing body of the City and its subsidiary organisations, and this has been recorded as the company's sector in its articles of association. As a central purchasing body, the company may put out to tender framework arrangements and dynamic purchasing systems through which the City and its subsidiary organisations can procure goods or services. Dustin Finland Oy was selected as the supplier of the telecommunications device installation service as a result of a tendering process.

DigiHelsinki Oy provides basic digital services as set out in a City-level framework agreement as well as accession agreements of individual user organisations (such as Divisions, agencies and municipal enterprises) and annual procurement decisions of individual user organisations. Exceptions from City-level services are to be arranged in individual user organisations' accession agreements. All Divisions of the City have concluded procurement contracts with the company that have been in force since 1 January 2023. There are differences in the delivery and scope of the services between the Divisions under the different contracts. Transferring the ICT service modules to the new company at once was considered challenging, which is why the transfer was phased, and KASKO retained some of its in-house ICT service provision and personnel.

Since the company started operating and the contracts with the individual Divisions were concluded, the situation where the provision of some services is shared between DigiHelsinki and the City's own organisation has persisted. In practice, the organisational changes have resulted in a transition period of around four years, during which many changes have taken place in the division of labour and responsibilities as well as in the personnel's tasks. During the transition phase, the division of tasks and responsibilities has become blurred, at least regarding some details. The VPN router used in the data breach was one such detail with ambiguously defined responsibilities (see section 2.1).

Private companies from which the City of Helsinki was already purchasing information management and information security services before the data breach were involved in managing the incident. Once the breach was detected, services were procured to investigate the incident and recover from it. The private operators involved in the incident are established and well-known ICT companies.

Telia Cygate maintains the firewall service used by the City of Helsinki and manages its logs. Telia Cygate Oy’s turnover in 2023 was approx. EUR 137 million, and it had around 400 employees.

Fujitsu Finland Oy offers, among other things, network and cloud service capacity to the City of Helsinki. It also provides services for passing on and integrating tickets produced by the City's subcontracting ICT service providers between different suppliers' information systems. Fujitsu Finland Oy’s turnover in 2024 was approx. EUR 300 million, and it had around 1,400 employees.

Dustin Finland Oy was commissioned by KASKO to maintain network devices. It performed remotely the annual certificate updates of Cisco's ASA 5515 VPN device that was hacked. Dustin Finland Oy's turnover in 2024 was approx. EUR 165 million, and it had around 220 employees.

Elisa Santa Monica Oy investigated the data breach on commission from the City of Helsinki from 3 May 2024 on. The company's cyber forensics team provides support for the investigation of and recovery from data breaches. The company engages in dozens of similar consultations each year. It also provides other security services, including Security Operations Center (SOC) services. Elisa Santa Monica Oy's turnover in 2023 was approx. EUR 64 million, and it had around 180 employees.

Palo Alto Networks Oy supplied firewalls to the City of Helsinki, while their management services were provided by Telia Cygate. After the data breach, Palo Alto Networks Oy analysed the firewall log data. Palo Alto Networks (Finland) Oy's turnover in 2024 was approx. EUR 9 million, and it had around 30 employees.

After the data breach, **Cisco Systems** has provided the City of Helsinki with expert services, especially in the analysis of fragmented log data and memory dumps of Cisco ASA 5515 VPN device. Cisco Systems Finland Oy's turnover in 2024 was approx. EUR 15 million, and it had around 55 employees.

	HELSINKI CITY GROUP			COMPANIES PROVIDING SERVICES TO THE CITY	
Actor's name	**City of Helsinki**	**Education Division as a division of the City of Helsinki**	**Service provider DigiHelsinki**	**Several companies**	**Company**
General description	Operator responsible for organisation	Sector-specific production task	Production of internal basic digital services for the city.	Companies providing various ICT services	Information security expert service
Before a data breach	• City-level development of the information management environment. • Administrative information security. • Developing the city's enterprise architecture. • Management of the Digital Foundation project. • DigiHelsinki Group steering.	• Responsibility for the implementation and development of information management in the sector. • Technical responsibilities of information management that have not been transferred to DigiHelsinki. • Partly administrative and partly technical information security tasks. • Unclear division of responsibilities with DigiHelsinki, especially with regard to technical maintenance.	• Information security management and maintenance in accordance with the agreements between the City and DigiHelsinki • Monitoring of communications in the internal network. • Technical information security in accordance with the agreements between the City and DigiHelsinki • Unclear responsibilities with the Education Division.	• Deliver and maintain ICT equipment and services purchased by the city or DigiHelsinki. • Ensure, for example, the technical information security, data protection and continuity management of these services.	Does not provide services
During a data breach	• **MiM** work begins. • Responsible for centralised communications at the city level.	• Identifying the data breach and launching prevention measures. • Notifications to the authorities, procurement of expert assistance and communication about the breach in the city organisation. • Launching **MIM** work.	• Participating in the technical implementation of management measures. • Breaking off the attach together with the Education Division.	The observation of the data breach is submitted to DigiHelsinki through one company.	• Establishing a situational picture and assisting in the efforts to end the attack. • The city submits a commission to the company after the data breach has been uncovered.
After a data breach	• Control and management of the situation. • Obligation to inform those subjected to the data breach. • Drawing up a development plan for improving information security.	Division-specific investigation measures, such as investigating network drive content.	Presenting and implementing development measures to improve information security.	• The necessary assistance related to the data breach investigation related to, for example, the forensic investigation of devices and the necessary log data. • Development of information security services.	• Producing the necessary new information security services. • Forensic investigation and reporting of the incident, drawing up recommendations.

Figure 10. Internal and external actors of the City of Helsinki and responsibilities in the data breach case.

2.8 Actions of the authorities

The **Ministry of Finance's** tasks include general development of information security in public administration. It also participates in developing the national cyber security strategy and legislation on information and cyber security. In recent years, the focus areas have included developing incident management and preparedness in shared ICT services as well as improving information security and data protection in critical sectors of society (Titukri). Together with other authorities, the Ministry of Finance develops the enhancement of manufactural situational awareness of cyber security in public administration and supports the development and use of the Digital and Population Data Services Agency's digital security and information services.

Ministry of Transport and Communications

The Ministry of Transport and Communications is responsible for legislation and strategy work related to the information security of telecommunications networks and services. The ministry's task is to enable well-functioning, secure and sustainable digitalisation, transport and communication solutions. The aim is to ensure and promote the trust of citizens, business life and public administration in the security of information society services. Among other things, this trust is based on user-friendly services, ensuring the protection of privacy and authenticity of content.

The Ministry of Transport and Communications prepares political and strategic guidelines and legislation falling within its remit, in addition to which the ministry is active in international forums. The ministry sees to well-functioning and secure connections, fair green and digital transition, and the preconditions for using data.

The Ministry of Transport and Communications is responsible for maintaining the national cooperation model for cyber security as set out in the Security Strategy for Society. The Finnish Transport and Communications Agency Traficom, which operates in the Ministry of Transport and Communications' administrative branch, is responsible for official duties relating to transport and communication. Traficom's Cyber Security Centre supports, guides and supervises information security and protection of privacy in electronic communication as well as maintains situational awareness of national cyber security.

The **Office of the National Cyber Security Director** is a unit that operates in conjunction with the Ministry of Transport and Communications but is separate from the ministry's departments. It is responsible for coordinating the development of national cyber security issues at Government level. It is responsible for the national coordination of the development, planning and preparedness of cyber security as well as the preparedness of critical ICT infrastructure at the strategic level. It also coordinates the follow-up of Finland's Cyber Security Strategy measures together with the ministries' monitoring group and its secretariat.

The **national information security authority** is the **Finnish Transport and Communications Agency Traficom**, which operates in the administrative branch of the Ministry of Transport and Communications. The **National Cyber Security Centre** is part of the Finnish Transport and Communications Agency Traficom, and its tasks are laid down in the Act on the Finnish Transport and Communications Agency[38].

The Cyber Security Centre supports, directs and supervises information security and protection of privacy in electronic communication. It maintains situational awareness of national cyber security. The Cyber Security Centre's operation promotes and safeguards the

[38] 936/2012.

security of information systems and telecommunications installations. The Cyber Security Centre is the authority responsible for the publicly regulated satellite service and the National Coordination Centre referred to in Article 6 of Regulation (EU) 2021/887 of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The Cyber Security Centre additionally ensures that the communications sector is prepared for incidents in normal conditions and emergencies, promotes and supervises the operational reliability of electronic communications, and supports society's general preparedness for incidents in normal conditions and emergencies in its sector. (1002/2021)

In addition, provisions on Traficom's duties relating to cyber security are laid down in section 304, subsection 1 of the Act on Electronic Communications Services (917/2014). Under paragraphs 1, 7, 8 and 10 of this section, in addition to those laid down elsewhere in the Act, the duties of Traficom are:

1) to promote the functionality, freedom from interference and security of electronic communications;

7) to collect information on violations of and threats to information security in respect of network services, communications services and added value services and on defects and interference situations in communications networks and services;

8) to disseminate information on information security matters and on the functioning of communications networks and services;

10) to investigate violations of and threats to information security directed at network services, communications services, added value services and data systems.

Based on these duties laid down by law, the statutory tasks of the CERT function also include form and sharing awareness of national cyber security situational awareness in order to investigate and prevent information security violations.

To fulfill its statutory duties, the Cyber Security Centre receives voluntary information security reports, which are classified according to the significance of the deviation and the scale of its impacts. The purpose of the classification is to produce an initial assessment of how critical the deviation is and how quickly it should be responded to, in the light of information provided by the notifier. Additionally, the reports enable the Centre to warn other actors, making it possible for them to improve the level of their cyber security.

The National Cyber Security Centre operates as the National Coordination Centre[39] and the national NIS point of contact between different authorities. Its tasks were expanded to implementing the NIS 2 Directive[40] that entered into force on 8 October 2024 under the national Act on Cyber Security[41], which entered into force on 8 April 2025.

The Act on Cyber Security[42] lays down provisions on the cyber security related tasks of the Cyber Security Centre's CSIRT unit. Under section 20, subsection 1 of the Act on Cyber Security, the tasks of the CSIRT unit include responding to deviation reports and, if necessary, assisting the reporting party in managing the deviation as well as collecting and analysing threat information and information relating to investigations of data breaches. In addition, the

[39] Regulation (EU) 2021/887 of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.
[40] NIS 2, or European Union Network and Information Security Directive.
[41] HE 243/2022.
[42] 124/2025.

Act on Cyber Security contains more detailed provisions on the Cyber Security Centre's competence and statutory tasks relating to providing HAVARO and Hyöky services.

In addition to the sections cited above, under section 303, subsection 1 of the Act on Electronic Communications Services (917/2014), Traficom has a duty is to supervise compliance with this Act and with the provisions and decisions issued under it, unless otherwise provided in the Act.

Among other things, the Act on Electronic Communications Services lays down provisions on the information security duties related to conveying electronic communications of telecommunications operators, corporate subscribers and other communications providers. In addition, the Act and the regulations issued by virtue of it contain a number of requirements concerning information security and preparedness in telecommunications operations. Within Traficom, the Cyber Security Centre's guidance and supervision department is responsible for directing and supervising operators in the context of these provisions and the regulations issued by virtue of them.

Additionally, the Finnish Transport and Communications Agency Traficom's Cyber Security Centre is the authority that oversees the public administration sector, certain operators in the digital infrastructure sector, digital service providers as well as actors providing ICT service management under the national Act on Cyber Security, which is based on the NIS2 Cyber Security Directive.

The National Cyber Security Centre develops and supervises the operational reliability and security of telecommunication networks and services and produces situational awareness of cyber security. The Centre publishes a monthly Cyber Weather report and a weekly review of current events.

The National Cyber Security Centre's customers can draw on its situational awareness information to organise and prioritise their preparedness activities. To maintain situational awareness, the Centre draws on the entire transport and communications sector of Traficom as well as national sources, including networks of organisations critical to security of supply and security authorities. Official international cooperation networks, or voluntary ones based on mutual trust, are also used.

Hyöky[43] is a service provided by the National Cyber Security Centre for public administration organisations and actors critical to the functioning of society that aims for surveying the attack surface of their public networks. A customer joining Hyöky provides the IP address spaces they use and at which the security survey is targeted. Hyöky reports are issued to the customer every few months or as needed.

The City of Helsinki joined the Hyöky service in late 2023. The investigation examined four Hyöky reports from 2023–2024. Critical and high-risk vulnerabilities came up in the reports.

KASKO only submitted the IP space of public services for the first survey. The purpose of this was to ensure that port scans do not cause undesirable side effects, including unwarranted alerts of network attacks. The hacked VPN router was not deemed to be part of the public service IP space, which is why its IP address was excluded from the survey.

If the VPN router had been included in the survey, it would have been flagged as a device detected in the report. The scan would have listed the server, allowing KASKO to notice that there was a 'forgotten' external device in the network.

[43] Attack surface survey service.

In connection with the data breach investigation, the Cyber Security Centre and the City of Helsinki carried out not only external Hyöky scans but also other, more comprehensive scans of the City's environment using different tools. Among other things, the Cyber Security Centre worked together with the different Divisions of the City to ensure that all IP address blocks in use were known. Several scans were performed on the blocks to detect any other potentially vulnerable targets. The scans also aimed to find out if the attacker had succeeded in expanding their access to the domains of the City's other divisions and if the attack was still active in the City's network environment, as well as to find any backdoors possibly set up by the attacker.

The Cyber Security Centre performed a separate scan of Finland's IP address space to determine if other organisations were using similar obsolete and vulnerable VPN devices.

Havaro (HAvainnointi and VAROitus, or monitoring and alerts) is a service intended to detect and give advance warning of serious data breaches. This information security service is provided by the Finnish Transport and Communications Agency (Traficom). Havaro monitors the client organisation's traffic and looks for signs of advanced attacks, such as foreign states' spyware and APT (Advanced Persistent Threat) activities.

The service is procured from a commercial security service center (SOC). The National Cyber Security Centre is responsible for its operation together with commercial actors' experts from the field. Actors critical to the security of supply and functioning of society as well as public administration actors can deploy the HAVARO service by installing the required sensor devices or software in their IT environments. The sensors attempt to detect and give alerts of threatening traffic. The Cyber Security Centre uses the data produced by the HAVARO service to investigate significant cyber incidents and to form national situational awareness of cyber security.

CERT (Computer Emergency Response Team) is a function of the National Cyber Security Centre aimed at preventing data breaches and providing information on information security issues. It also supports technical investigations of serious security breaches.

A **report on an information security incident** can be submitted to the National Cyber Security Centre using an online form. The reports are classified and recorded in statistics. The classification criteria include the number of people and actors affected by the incident, the importance of the target for society, and the urgency of the need for measures. After classification, the measures that may need to be taken on the basis of the report are assessed.

The National Cyber Security Centre offers by 24/7. During the night, emergency service relies on a standby arrangement that is able to respond to serious situations if necessary.

The National Cyber Security Centre's role in information security violations is mainly limited to assisting and supporting the targeted actor. The purpose of the assistance, support and advice it provides is to promote the investigation and prevention of security breaches and recovery from them. The scope of the assistance or support is not predetermined, and it depends on such factors as the resources available at the time. The extent to which the actor is able to handle and investigate the violation themselves also influences the matter. To perform its statutory duties to investigate data breaches in exceptional cases, such as the data breach targeting the City of Helsinki, the Cyber Security Centre's experts can also assist a customer with managing the breach in concrete terms (DFIR, Digital Forensics & Incident Response).

There may be major differences between the resources of actors affected by security breaches, which means that the need for official assistance may vary significantly. At the time

of the data breach case in question, the National Cyber Security Centre did not have a general process description for investigating security breaches.

Preparedness for investigating and preventing security breaches in Finland is based on extensive cooperation and communication between the authorities, information security companies and other actors. The National Cyber Security Centre serves as an umbrella organisation that promotes the activities. Its assistance services are free of charge for the affected organisation.

In the context of coordinating national cyber security, the Cyber Security Centre coordinates Information Sharing and Analysis Centres (ISACs)[44], which are cyber security cooperation bodies established in different sectors. The ISACs discuss confidentially cyber security issues, including threats, phenomena and good practices. There are also separate centres for municipalities and the central government.

The **Finnish National Agency for Education**, which operates under the Ministry of Education and Culture, is responsible for developing, steering and evaluating education and early childhood education and care. Its tasks include preparing curricula and qualification requirements, achieving education policy objectives and developing measures that promote the quality and equality of education. The Finnish National Agency for Education supports educational institutions, teachers and students by offering instructions, materials and funding. It is also responsible for international cooperation in education and participates in developing the Finnish education system.

The Finnish National Agency for Education has prepared extensive guidelines for the education and cultural administration on data processing, data protection and information security for schools and day-care centres. The material has been prepared in cooperation with the Data Protection Ombudsman. On 15 October 2021, the Data Protection Ombudsman made an initiative to the Finnish National Agency for Education on developing the use of personal data in information systems for education. The measures referred to in the initiative have not been completed.

The **Information Management Board** is a special authority established in connection with the Ministry of Finance to assess and promote compliance with the requirements and practices laid down in the information management legislation. The Information Management Board consists of public administration representatives. It has members from key authorities that steer information management and apply the Information Management Act. Every two years, the Information Management Board draws up a report on the findings of the evaluations it conducts. The reports contain recommendations addressed at the Ministry of Finance. The Information Management Board is not competent to assess compliance with the information security requirements laid down in chapter 4 of the Information Management Act.

In its evaluation report, the Information Management Board has drawn attention to the fact that information management steering tasks are divided between several different authorities and that they overlap.[45] In addition to the Information Management Board, the authorities that issue recommendations on information security or share best practices include at least the National Cyber Security Centre, National Emergency Supply Agency and Digital and

[44] ISAC groups, Information Sharing and Analysis Centre https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups

[45] Information Management Boards' evaluation report 2022–2023 p. 42. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165453/VM_2024_16.pdf

Population Data Services Agency's digital security services. The Ministry for Foreign Affairs, the National Emergency Supply Agency and the National Archives of Finland also have tasks relevant to this theme.

Figure 11. Authorities relevant to the steering of general legislation on information management. (Figure: Information Management Board)

Following its supervision plan, the Information Management Board evaluated the activities of the City of Helsinki in 2020–2023 as part of its normal work targeting local governments. This supervision comprises oversight of legality and is mainly carried out by means of requests for information and queries. No actual monitoring visit was made to the City of Helsinki. Based on the evaluations carried out, there were no shortcomings in compliance with the obligations laid down in the Information Management Act in the City of Helsinki.

Helsinki Police Department is the largest police unit in Finland. It employs around 1,600 people, of whom some 1,300 are police officers. The unit operates in the City of Helsinki area and performs local police duties. The unit is additionally responsible for the safety of the President of the Republic, members of the Government and state visitors. The national police preparedness unit Karhu, the national investigation team of human trafficking and the Traffic Safety Centre are also co-located with Helsinki Police Department.

The police department is responsible for pre-trial investigations of offences committed in its area unless the police organisation's division of labour dictates otherwise. Helsinki Police Department received the report of an offence made by the City of Helsinki through its electronic reporting system. The report of an offence was pre-processed, and an investigator and head investigator were appointed for it.

As pre-trial investigation measures, the Police Department acquired information from the City of Helsinki and published a press release on the launch of the pre-trial investigation. The Police Department also initiated cooperation with the National Bureau of Investigation.

The **National Bureau of Investigation** is a national special unit of the Finnish police administration that operates across Finland. The National Bureau of Investigation has special expertise in combating organised crime, narcotics crime, economic crime and cybercrime, among other things. It works in international cooperation with the authorities of other countries and coordinates Finland's participation in Europol and Interpol activities. The National Bureau of Investigation supports local police units in complex criminal investigations and contributes to maintaining national security.

The National Bureau of Investigation engages in collaboration with the local police in which the local police take care of matters related to injured parties, while the National Bureau of Investigation handles forensic investigations and international cooperation. The head investigator in this case represents the National Bureau of Investigation.

The measures taken by the National Bureau of Investigation regarding the data breach in Helsinki are linked to the pre-trial investigation. In this respect, police activities in cybercrime cases differ from those in other types of crime, as the possibilities of the police to stop crimes being committed in information networks are rather limited.

Once the breach was detected, other actors' measures helped to restore the secure state of KASKO's network. The police do not have operational capabilities for taking possession of network environments, starting their surveillance or removing a hacker from a network. Such actions must be performed by the organisation that has been attacked or the service providers it uses.

The investigation of cybercrimes and realisation of criminal liability usually require significant international cooperation and contacts, which are the responsibility of the National Bureau of Investigation.

On 13 March 2025, the National Bureau of Investigation reported that it suspected a data protection offence associated with the data breach targeting the City of Helsinki, in which it initiated a pre-trial investigation. The investigation will determine if the City had protected the data adequately.

The **Finnish Security and Intelligence Service** prevents and combats the most serious threats to national security, including terrorism and illegal intelligence activities of foreign states in Finland. As a result of the coronavirus pandemic and digitalisation, companies and society have increasingly introduced online functions, which has also increased the role of the Internet in the intelligence activities of the Finnish Security and Intelligence Service. In the data breach investigation, the Finnish Security and Intelligence Service mainly monitored the progress of the pre-trial investigation.

The **Data Protection Ombudsman** is an independent authority that supervises the processing of personal data and enforces compliance with the General Data Protection Regulation and other special legislation on personal data processing. The Data Protection Ombudsman provides advice on data protection matters, handles complaints related to data protection violations, and may impose penalties. The Data Protection Ombudsman has the right to inspect organisations' data protection practices. In addition to the Ombudsman, two Deputy Data Protection Ombudsmen and around 60 other officials work in the Office of the Data Protection Ombudsman.

After detecting a data breach, the controller is obliged to notify it to the Data Protection Ombudsman within 72 hours. The Office of the Data Protection Ombudsman starts investigating the case on the basis of the notification.

The Data Protection Ombudsman has investigated the data breach targeting the City of Helsinki following the provisions on processing administrative matters and will issue a decision on the matter later. The Data Protection Ombudsman's supervisory activities comprise oversight of legality carried out following the procedure for processing an administrative matter in the order laid down in the Administrative Procedure Act.

The Data Protection Ombudsman received a notification of the data breach from the City of Helsinki after the breach had been detected on 30 April 2024 and began investigating the matter on this basis. The City of Helsinki complemented its notification several times as the internal investigation progressed and in response to information requests received from the Office of the Data Protection Ombudsman. The Data Protection Ombudsman provided the City of Helsinki with advice relating to compliance with the General Data Protection Regulation, including fulfilling the information obligation associated with a data breach.

In addition, the Data Protection Ombudsman supported the City of Helsinki's communication actions and was contacted by persons whose data may have been contained in the dataset affected by the breach.

The **Association of Finnish Local and Regional Authorities** is a registered association of the municipalities. Regional councils, joint municipal authorities and limited companies associated with local governments are also involved in its work. The Association is the joint representative of the local government sector that employs around 140 people in its organisation. Its subsidiaries are FCG Finnish Consulting Group Oy, KL-Kuntahankinnat Oy and KL-Kustannus Oy. The Association of Finnish Local and Regional Authorities represents the municipalities' interests in all matters relevant to local government. These matters also include early childhood education, basic and secondary education as well as digitalisation, cyber security and data protection issues in municipalities. The Association supports municipalities' peer development and networking in the field of information management, information security and data protection, for example by maintaining networks of municipalities' information security and data protection officers as well as by offering consultations to its members. FCG additionally organises topical digital security events and courses for local government actors for a fee.

Guidance and advice are emphasised in the **authorities' preventive activities**, with the aim of ensuring that the actor has identified their key responsibilities in the processing of personal data and information management. Regular supervision of compliance with these obligations is very limited. The oversight of the Information Management Board mainly aims to describe the fulfilment of information management obligations at the national level. The Data Protection Ombudsman conducts control visits, both planned and unannounced ones. The fulfilment of the responsibilities may mainly be evaluated afterwards in the context of various data protection violations or complaints regarding activities.

The Hyöky and HAVARO services maintained on public funds have been successful in identifying and preventing threats and vulnerabilities which the user organisation or the information security service provider it relies on have not noticed. However, the services are not widely used in the public sector. They are also in need of technical development.

Measures that prevent offences and ensure that criminal liability is realised are the key to fighting crime. These measures require international cooperation. National projects aiming to develop the fight against cybercrime are also significant.

At the centre of managing a data breach incident is the organisation whose data the breach targets. A precondition for this is that the organisation's technical and administrative

safeguards are proportionate to the information security risks and that is has an ability to detect and prevent an attempted data breach. In addition, the organisation must ensure in advance that it has the necessary competence to prevent and investigate a data breach and manage an incident if necessary. The organisation that manages the data is also responsible for informing the victims of a data breach.

By means of advance preparations, the organisation can ensure that it has access to assistance and sufficient expertise for investigating and managing a data breach. There are several companies providing such DFIR (Digital Forensics & Incident Response) services in Finland. To investigate a criminal offence, knowledge of the organisation and its information system environment is needed, which the pre-trial investigation authorities do not have. This is why investigations carried out by the organisation itself or outsourced to a company play a key role in investigating the offence.

Several different (local, national and international) authorities participate in investigating a data breach as indicated by their roles. The most extensive free expert assistance supporting a victim of a data breach is provided by the National Cyber Security Centre.

The legislation does not specify which authority should take command in **cases of data breach**, whereas in accidents and offences in the real world, the responsibility for overall command is typically divided between the rescue and police authorities. The incident management model differs from the above and complies with the division of responsibilities for risk management, in which the actor is also responsible for handling deviations and incidents fairly independently.

The national cyber security cooperation model in Finland is decentralised, and its principles are similar to those of the comprehensive security cooperation model. In the cyber security cooperation model, each competent authority takes command of incident management within the limits of its duties and competence. Maintaining the cyber security cooperation model is one of the strategic tasks of the Security strategy for society, and its aim is to ensure close preparedness cooperation between key actors in society in all circumstances.

Under the Act on Cyber Security, a plan in which the available capabilities, resources and procedures are itemised is drawn up for responding to and managing large-scale cyber security deviations and crises. This also includes the requisite information on the authorities' duties and responsibilities.

In keeping with the comprehensive security model, the management of incidents that threaten society's vital functions relies on cooperation between the authorities, local government, different branches of administration, ministries and businesses that is as comprehensive as possible, as well as support provided for other security-related actors. This model also applies to the management of cyber incidents, in which several authorities have their tasks depending on the stage of the incident. Traficom's Cyber Security Centre is responsible for investigating and coordinating measures in the initial phase of a cyber incident reported to it. As the organisation targeted by the cyber incident makes a report of an offence regarding the incident, the responsibility for leadership and investigation is transferred to the police. The competent authority leads the operative measures, initiates actions relating to managing the incident, is responsible for communication, and disseminates information about the situation following agreed practices.

Legislation on combating cyber security incidents is about to be amended. For example, cooperation between the authorities in managing large-scale cyber security incidents and crises will be reviewed.

	MINISTRY OF TRANSPORT AND COMMUNICATIONS' ADMINISTRATIVE BRANCH	MINISTRY OF THE INTERIOR'S ADMINISTRATIVE BRANCH			OTHER AUTHORITIES
Actor's name	**Traficom's National Cyber Security Centre**	**Helsinki Police Department**	**National Bureau of Investigation**	**Finnish Security and Intelligence Service**	**Office of the Data Protection Ombudsman**
General description	The task of the National Cyber Security Centre's CERT (Computer Emergency Response Team) is preventing data breaches and providing information on information security issues.	Pre-trial investigation authorities		National security	National data protection authority
Before a data breach	• Situational awareness and networking service, surveillance and assistance • Maintains partnerships and international relations to perform its tasks. • Attacks surface mapping (scanning) and prevention of attacks. • Constant monitoring of serious information security threats within the client's network.		• Projects on preventing cyber crime. • International information exchanges and fight against crime.	Detects, prevents and uncovers actions, projects and offences that may threaten the form of government or public order, or Finland's internal or external security	Supervises compliance with data protection legislation and other acts on personal data processing, promotes awareness of the risks, rules, protection measures, obligations and rights related to personal data processing, conducts studies and inspections, imposes administrative penalties for GDPR infringements
During a data breach	• Supports the targeted organisation and provides expert assistance. • Data breach detection and initiation of counter-measures.	• Receives reports of an offence from the area for which it is responsible. • Launches a pre-trial investigation. • Works together with the National Bureau of Investigation.	Participates in and supports the pre-trial investigation.	Provides expert assistance if the situation so requires.	• Receives notifications of a data breach involving personal data. • Provides expert assistance if the situation so requires.
After a data breach	• Hyöky scans. • Gathers and passes on information nationally and internationally. • Issues proposals for developing information security measures. • Support for data breach detection and initiation of countermeasures. • If needed, DFIR investigation	• Duty to conduct a pre-trial investigation. • Investigation measures. • Liaises with injured parties in the data breach. • Leadership of pre-trial investigation transferred to the National Bureau of Investigation.	• Questions with an international dimension for identifying and reaching the perpetrator. • Forensic investigations. • Communication about the investigation.	Significance of the data breach for national security.	• Supervises the rights of data breach victims. • Imposes any administrative penalties for GDPR infringements.

Figure 12. Public actors and authorities and their responsibilities in data breach cases.

2.9 Statutes, regulations and guidance

This chapter discusses the regulations, instructions and recommendations issued by actors external to the City of Helsinki.

Under section 8 of the **Municipalities Act**[46], the municipality is responsible for organising its statutory services. This responsibility includes ensuring equality of service availability, definition of need, quantity and quality, method of provision, monitoring of provision, exercise of the powers of a public authority, and financial responsibility for the tasks.

Under the Municipalities Act, the City of Helsinki is responsible for organising early childhood education and care, basic education, general upper secondary education and vocational education and training. Further provisions on these tasks are laid down in special legislation, including the Act on Early Childhood Education and Care[47], Basic Education Act[48], Act on General Upper Secondary Education[49] and the Act on Vocational Education and Training[50].

[46] 410/2015.
[47] 540/2018.
[48] 628/1998.
[49] 714/2018.
[50] 531/2017.

Section 2, subsection 3 of the **Constitution of Finland**[51] lays down the principle of administration being subject to law, which safeguards the rights of those bringing a matter before the authorities. According to this subsection, the exercise of public authority must be based on law, and law must also be strictly observed in all public activity. In statutory services, however, the possibilities the customer of the administration has to influence the processing of their matter or data are limited, which is why the authorities' actions play a key role in the realisation of legal protection.

The principle of the public administration being subject to law is emphasised by the provision on liability for acts in office laid down in section 118 of the Constitution, under which a civil servant is responsible for the lawfulness of his or her official actions. This accountability is complemented by the Criminal Code[52], chapter 40 of which contains provisions on offences in public office, including violation of official duty referred to in chapter 40, section 9 as well as negligent violation of official duty referred to in section 10 of this chapter. When the Data Protection Act[53] was enacted, the legality requirement applicable to public administration and the official's liability for acts in office were considered one of the grounds for not applying administrative penalty fees to authorities.[54]

The fundamental principles of good administration laid down in chapter 2 of the **Administrative Procedure Act**[55] safeguard the rights of people dealing with the authorities. They include the requirement of equal and impartial treatment and only exercising the authority's competence for purposes acceptable under the law. Other requirements include the service principle, obligation to provide information and advice, requirement of appropriate and clear language, and inter-authority cooperation. Customers of the public administration are also safeguarded by the procedural rules of the Administrative Procedure Act and the possibility of appealing decisions or filing an administrative complaint. The Parliamentary Ombudsman and the Chancellor of Justice also oversee the legality of the authorities' and public officials' activities and ensure that they fulfil their obligations.

Under section 90 of the **Municipalities Act**[56], each municipality and joint municipal authority must have administrative regulations. Pursuant to this Act, the administrative regulations must contain the necessary stipulations on at least the arrangement of the municipality's administration and activities, decision-making and administrative procedures, and the activities of the municipal executive.

Among other things, the City of Helsinki's Administrative Regulations oblige the City Board to ensure that the instructions, practices, responsibilities and supervision relating to information management and document management are specified (Chapter 24, section 3). The Administrative Regulations further stipulate that directing information management and document management is the responsibility of the Administration Department of the City Executive Office, while that steering information management is the responsibility of the Strategy Department of the City Executive Office.

Regulation on data protection and document management

Article 8 of the **Charter of Fundamental Rights of the European Union** safeguards the protection of personal data as a separate fundamental right, while Article 7 of the Charter

[51] 731/1999.
[52] 39/1889.
[53] 1050/2018.
[54] HE 9/2018 vp pp. 56–56.
[55] 434/2003.
[56] 410/2015.

safeguards respect for private and family life. Personal data are also safeguarded by Article 8 on the right to respect for private and family life of the European Convention on Human Rights, the right to private and family life enshrined in Article 17 of the International Covenant on Civil and Political Rights, and the right to privacy laid down in section 10 and the obligation to guarantee fundamental rights and liberties and human rights laid down in section 22 of the Constitution of Finland. The protection of personal data also covers personal data that are not within the scope of privacy.

Many changes have taken place in the legislation on data protection, information security and the processing of personal data in 2018–2025.

The **European Union General Data Protection Regulation**[57] (GDPR) has been applicable from 25 May 2018. In order to implement the GDPR, several statutes were amended in Finland, the most important change being the passing of the Data Protection Act and repealing of the Personal Data Act[58].

The General Data Protection Regulation contains provisions on the processing of personal data and their free movement. Pursuant to Article 2 GDPR, the Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Most parts of the GDPR comprise mandatory regulation that cannot be altered by national legislation. This is why the Data Protection Act does not provide a comprehensive understanding of what data protection contains. The Finnish Data Protection Act only contains provisions on matters for the part of which national regulation is required, or at least permitted, under the GDPR.

Personal data refers to any information relating to an identified or identifiable natural person (*data subject*). In addition to direct identifiers, this includes data on how a certain individual can be identified, for example with the help of additional information. A *controller* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines* the purposes and means of the processing of personal data. The controller may also be determined pursuant to legislation.

The City of Helsinki is the controller with respect to the personal data it has processed for the purposes of its activities, either by specifying the purpose and means of the processing itself or by processing personal data to comply with its legal obligation. The GDPR imposes a number of obligations for data processing on the controller.

The **Act on Information Management in Public Administration**[59] (Information Management Act) also applies to information management and use of information by public authorities. The purpose of the Act is to ensure harmonised and high-quality management and secure processing of datasets of authorities in order to implement the principle of openness as well as to promote the interoperability of information systems and information pools. Under section 3 of the Information Management Act, the Act applies to information management and the use of information systems when authorities process datasets. Section 2 of the Information Management Act defines the concepts used in the Act. Under section 4, subsection 1 of the Information Management Act, municipalities and joint municipal authorities are information management entities referred to in the Act. Before the

[57] (EU) 2016/679.
[58] 524/1999.
[59] 609/2019.

Information Management Act entered into force, provisions on processing datasets and information management in public administration were not contained in a single general statute. Even after the entry into force of the Act, provisions on the authorities' responsibilities relating to information management also continue to be contained in other general statutes on the administration, including the Act on the Openness of Government Activities, the Archives Act and the General Data Protection Regulation. The introduction of the Act necessitated significant reforms on the part of the information management entities.

The **Act on the Openness of Government Activities**[60] contains provisions on the authorities' obligations to promote publicity and openness as well as on the legal preconditions for restricting them. Section 24 of the Act on the Openness of Government Activities contains provisions on secret information, among other things. The organisational scope of the Information Management Act is laid down in the Act on the Openness of Government Activities.

The **Archives Act**[61] lays down the obligations of a records creator. Under section 7 of the Archives Act, the task of archiving is to ensure the usability and preservation of documents, to provide information services related to documents, to determine the preservation value of documents, and to destroy unnecessary documents. Archiving must support the realisation of the openness principle, taking into account the legal protection of private individuals and corporations as well as data protection. The City of Helsinki is a *records creator*, and under section 9 of the Archives Act, the City Board is responsible for the arrangements of its archival function.

Under section 7 of the **Administrative Procedure Act**, service and the consideration of matters by an authority should be arranged so that the customer of the administration receives appropriate service and that the authority can perform its tasks productively.

Figure 13. Regulatory environment of information management, information security and data protection.

[60] 621/1999.
[61] 831/1994.

Data protection requirements

The **General Data Protection Regulation** lays down a wide range of conditions on the processing of personal data and imposes many types of obligations on the controller. Firstly, there must always be grounds for processing laid down in the General Data Protection Regulation. The general grounds for processing personal data are laid down in Article 6 GDPR, which is supplemented by section 4 of the Data Protection Act. In the case of authorities, the grounds for processing usually include the controller's legal obligation, performance of a task carried out in the public interest, or the exercise of official authority. Consent, performance of a contract and protection of a vital interest are also possible grounds for processing.

Article 9 GDPR lays down provisions on the processing of special categories of personal data. Special categories of personal data include data concerning ethnic origin, political opinion, religious or philosophical beliefs and health. For example, schoolchildren's religious beliefs and health data consequently belong to the special categories of personal data.

Whereas the processing of special categories of personal data is prohibited as a rule, there are several exceptions to the prohibition. For example, their processing is permitted when it is directly due to a legal obligation of the controller, such as organising early childhood education and care and basic education. According to the provisions of the Data Protection Act, the controller and the processor must take suitable and specific measures to safeguard the rights of the data subject when processing special categories of personal data. They include

- measures that enable subsequent checking and verification of the identity of the person who has recorded, altered or transferred personal data
- measures to improve the competence of the personnel processing personal data
- designation of a data protection officer
- internal measures by the controller and the processor for preventing access to personal data
- pseudonymisation of personal data
- encryption of personal data
- measures that ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing
- specific rules of procedure for ensuring compliance with the Data Protection Regulation and this Act when personal data are transferred or processed for another purpose
- a data protection impact assessment in accordance with Article 35 of the Data Protection Regulation
- other technical, procedural and organisational measures.

Separate provisions on processing relating to **criminal convictions and offences** are contained in Article 10 GDPR and section 7 of the Data Protection Act.

Article 5(1) GDPR sets out the principles which must be followed whenever personal data are processed. According to paragraph 2 of this Article, the controller shall be responsible for, and be able to *demonstrate* compliance with, these principles (accountability).

According to the data protection principles, personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- limited to what is necessary in relation to the purposes for which they are processed
- kept up to date as necessary; inaccurate personal data must be erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security and confidentiality of the personal data.

Article 24 **GDPR** contains provisions on what the controller must do to ensure and demonstrate that the processing of personal data is lawful. According to paragraph 1 of this Article, the controller must implement appropriate *technical* and *organisational* measures to *ensure* and *demonstrate* that processing is performed in accordance with the GDPR. The technical and organisational measures required at any given time are assessed taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. For special categories of personal data, more detailed processes and stronger security measures are required than, for example, for personal data that do not contain data within the scope of the data subject's private life. The required measures are also subject to the data protection principles laid down in Article 5(1) GDPR.

Technical security measures include controlling access to hardware and systems, preventing unauthorised access to data and systems, logging events, controlling the source and routing of traffic, determining access rights to systems, appropriate organisation of maintenance activities, and protecting data and systems from acts or events that put their security at risk, including viruses and other malware. Where necessary an information system must, for example, be protected ensuring that even attempts to unlawfully access personal data trigger an alert to the controller.

Organisational measures include organisational arrangements, definitions of personnel's tasks and responsibilities as well as instructions, training and supervision. For example, the controller must ensure that a user's rights correspond to their position and responsibilities and that the user can only access data that they need to perform their duties. The more sensitive the data, the more limited the rights to process them must be. If necessary, procedures must also be created, including a log information system, that can be used to monitor the use and disclosures of data.

It is not adequate to arrange for the technical and organisational measures once and then forget all about them, as these measures must be reviewed regularly and updated when needed.

The controller's *accountability* is based on both Article 5(2) GDPR and Article 24(1) GDPR. Firstly, preparedness for the accountability obligation 'forces' the controller to consider and document its processes, in which case shortcomings may be noticed that can be remedied before actual damage has occurred. Secondly, the accountability obligation allows the controller to show that they have actively sought to identify data protection risks and put in place the necessary measures to protect personal data. Failure to comply with the accountability obligation violates the GDPR even if no other concrete data protection infringement had occurred.

Accountability also means a *duty to document*, which is in practice fulfilled by taking certain measures and keeping a record of them. The scope of accountability depends, among other things, on the size of the organisation and the amount and quality of personal data. For example, compliance with the accountability obligation may take the form of a privacy statement, data protection policies as well as internal and external guidelines, information practices, assessments of the legal ground for processing, documentation of impact assessments and prior consultations, documentation of data breaches and the ensuing processes, documentation of the data protection officer's status and tasks, data processing agreements, definition of joint controllers' responsibilities, as well as documentation of transfers of personal data to third countries.

The GDPR also contains provisions on the security of personal data processing. Article 25 GDPR provides for *data protection by design and default*, which aim to address data protection already when designing information systems and planning processing operations, not only when the information system or service is already technically finished. It is easier to integrate data protection and information security measures into the activities in the design phase than to attempt to modify the finished system or practice afterwards to improve its security.

According to this provision the controller must – taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself – implement appropriate technical and organisational measures. To comply with the principle of data minimisation, it is specifically provided that the controller must implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. The Article also states that the controller must ensure, in particular, that by default personal data are not made accessible to an indefinite number of natural persons.

The **adequacy of information security and data protection measures** must be continuously assessed and updated, for example when the processing measures change or technology advances. The controller must also assess the actions of the processors it uses and strive to ensure that their actions are lawful.

Information security refers to protecting data, services, systems and telecommunications, ensuring that the data can only be accessed by those entitled to do so, that the data can only be modified by persons entitled to do so, and that the data and information systems are available for those entitled to use them. Article 32 GRDP lays down provisions on the *security of processing.* Under this Article, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

When assessing the adequacy of measures, the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons must be taken into account. The measures intended here may include the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In practice, these measures may include controlling access to hardware and systems, preventing unauthorised access to data and systems, logging processing events, controlling the source and routing of traffic, determining access rights to systems, appropriate organisation of maintenance activities, and protecting data and systems from acts or events that put their security at risk, including hacking, viruses and other malware.

The provision further points out that the controller and processor must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. The preconditions for this include providing the personnel with training and instructions. The precondition for providing instructions further is that the controller knows what data are processed in its operations and why, and that data protection and information security aspects have been taken into account when organising the processing.

Article 35 GDPR lays down provisions on data protection *impact assessment*. According to this Article, where a type of processing in particular using new technologies – taking into account the nature, scope, context and purposes of the processing – is likely to result in a high risk to the rights and freedoms of natural persons, the controller must prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The purpose of the impact assessment is to help identify, assess and manage the risks involved in the processing of personal data. It also helps the controller comply with the data protection legislation as well as document and demonstrate their compliance. In particular, this assessment is required when processing on a large scale special categories of data referred to in Article 9(1), which include data concerning religion and health. The impact assessment must be carried out before the start of the processing and updated where necessary. The Data Protection Ombudsman has illustrated the risk formation with the following figure (Figure 14):

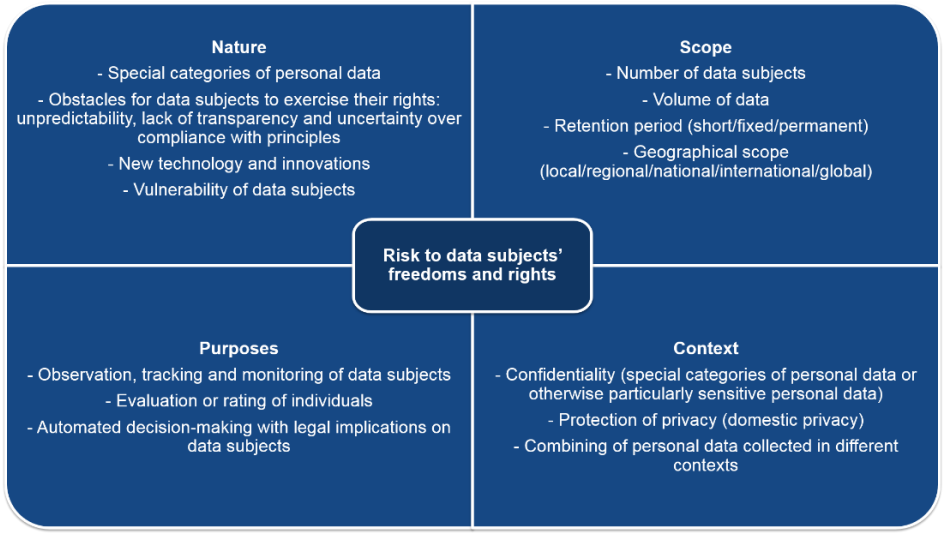

Figure 14. Risk formation in data processing. (Figure: Office of the Data Protection Ombudsman)[62]

[62] Office of the Data Protection Ombudsman: Risk assessment and data protection planning. 26 February 2025 https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning

The GDPR provides that in the case of a *personal data breach*, the controller must not later than 72 hours after having become aware of it *notify* the supervisory authority and also communicate the data breach to the data subjects if it is likely to result in a risk to the rights and freedoms of natural persons. The purpose of these notifications is to determine if a data breach has occurred but also to initiate precautions with the aim of reducing the potential for misuse of the data (Articles 33 and 34).

The obligation to designate a *Data Protection Officer* is laid down in Article 37 GDPR. Pursuant to this provision, the City of Helsinki must have a designated Data Protection Officer.

Information security requirements laid down in the Information Management Act

The **Act on Information Management in Public Administration** contains provisions on organising and describing information management, interoperability of information pools, and implementation of the interoperability of information systems, technical interfaces, viewing access and information security that apply to the entire public administration.

Section 13 of the Act imposes the following legal requirements concerning information security on authorities:

- An information management entity must monitor the state of the information security of its operating environment and ensure the security of its datasets and information systems over their entire lifecycle. The information management entity must determine the material risks to data processing and dimension the information security measures in accordance with the risk assessment.
- The resilience and operational availability of the information systems that are material with regard to performance of the tasks of the authorities must be ensured with adequate testing on a regular basis.
- The authority must plan the information systems, the internal structure of the information pools and related processing so that the publicity of documents can be easily implemented.
- In its procurements, the authority must ensure that appropriate data security measures have been implemented in the information system to be acquired.
- Separate provisions are laid down on the assessment of the information security of the information systems and telecommunications arrangements of the authorities.

These requirements are basic premises. They do not contain detailed provisions on how or by what methods information security must be ensured.

Katakri 2020 is an information security audit tool for authorities that can be used to assess an organisation's ability to protect secret information. The first Katakri set of national security audit criteria was completed as early as 2009. The Katakri criteria are divided into three areas:

- The section on *security management* aims to ensure that the organisation has an effective information security management system and adequate personnel security procedures for protecting classified information.
- The section on *physical security* describes the security requirements for the physical environment in which classified information is used.
- The *technical security* section describes the security requirements for the technical environment in which information is processed.

- **Cybermeter (Kybermittari)**[63] is a set of indicators based on international measurement models for cyber security capabilities. The Cybermeter, which has been customised for companies and organisations operating in Finland, helps improve the ability of companies and organisations, and society at large, to control cyber risks. The Cybermeter provides the managers and information security professionals of companies and organisations with a concrete tool for better management of cyber threats.

Assessment criteria for information security in public administration (Julkri)[64] is a recommendation issued by the Information Management Board. It supports the development and evaluation of information security in public administration. It can also be used to support assessments of compliance with the information security requirements laid down in the Information Management Act, the Security Classification Decree and partly also the General Data Protection Regulation. Its section on data protection was prepared in cooperation with the Office of the Data Protection Ombudsman.

ISO/IEC 27001 is the most widely recognised international standard for information security management systems. It defines requirements for the establishment, implementation, maintenance, monitoring and improvement of an organisation's information security management system. It helps organisations draw up a security management policy, implement the necessary controls and set clear targets for improving security.

Section 15 of the **Information Management Act** contains provisions on ensuring dataset security. This includes ascertaining that the unaltered state of datasets has been sufficiently ensured; datasets have been protected against technical and physical damage; the authenticity, timeliness and accuracy of datasets have been ensured; the availability and usability of its datasets have been ensured; the availability of datasets is restricted only if access to the information or processing rights have been separately restricted in the law; and the datasets can be archived as required. The Act also requires that the datasets be processed and stored on premises which are sufficiently secure with a view to implementing the requirements relating to the reliability, integrity and availability of datasets.

Under section 16 of the Information Management Act, the authority in charge of the information system determines the access rights to the system in accordance with the needs relating to the tasks of the user and keeps them up to date.

Under section 17 of the Information Management Act, an authority must ensure that the necessary log data are compiled of the use of its information systems if the use of the information system requires identification or other login. The purpose of collecting the log data is to monitor the use and disclosures of the data in the information systems and to investigate technical errors in systems.

Information management and data lifecycle

Under section 5 of the Information Management Act, an information management entity must maintain an *information management model* which defines and describes information management in its operating environment. The information management model is maintained to design and implement the management of services, consideration and datasets, to implement the rights and restrictions relating to access to information, to decrease multiple

[63] Cybermeter https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter

[64] Julkri; Publications of the Ministry of Finance 2023:46.

collection of information, to implement the interoperability of information systems and information pools, and to maintain information security.

Under section 26 of the Information Management Act, an information management entity must form a case identifier specifying a matter admitted or submitted to be considered by an authority with which the information relating to the matter is specified. This provision is specifically related to the processing of administrative matters which, in the context of the case to be investigated, include making decisions concerning the personnel, student admissions, support provided for a student and payment obligation.

Section 27 of the Information Management Act contains provisions on datasets that are generated in connection with services other than the actual consideration process of a matter (management of datasets in service production). This provision covers all other datasets produced or generated by an authority that are not processed in a logical case register. The data affected by the data breach were mainly within the scope of this provision.

The information management entity must arrange the management of datasets generated in connection with other than the consideration of a matter so that the documents composed of the dataset can be searched with an identifier specifying the sets of data so that the information can be easily provided to the party entitled to it. The authority must, without delay, register the documents and other information generated in service production so that their generation in service production can be verified afterwards. Before the Information Management Act was passed, there was no corresponding provision on information management in services in Finland[65]. The Information Management Board has issued a more specific recommendation on information management in services and its development.

Under section 21 of the Information Management Act, the controller must specify a retention period for each dataset. After the end of the retention period, the datasets must be destroyed. Any data that must be archived by law or whose preservation is deemed to be necessary on other grounds are archived as laid down in the Archives Act.

There are no specific provisions on the names or contents of personal data files used in education, excluding the student welfare register, on which provisions are laid down in the Student Welfare Act[66]. Consequently, general regulation on information management, data protection and openness are to a large extent followed in information processing in the education sector.

Under the Archives Act, the task of archiving is to ensure the usability and preservation of documents, to provide information services related to documents, to determine the preservation value of documents and to destroy unnecessary documents. An information management plan is maintained for the purpose of records creation. The information management plan is a plan linked to the information management model.

The data must be destroyed when the retention period specified for them has expired or the need to use the data has otherwise ended. General instructions on retention periods are based on storage period instructions and similar.[67]

---

[65] HE 248/2028 vp. Government proposal to Parliament on the Act on Information Management in Public Administration.
[66] 1287/2013.
[67] Kunnallisten asiakirjojen säilytysajat. Määräykset ja suositukset (Retention periods of local government documents. Regulations and recommendations) Education Division 12. 25 February 2025 https://www.kuntaliitto.fi/julkaisut/2002/1349-kunnallisten-asiakirjojen-sailytysajat-maaraykset-ja-suositukset-opetustoimi-12

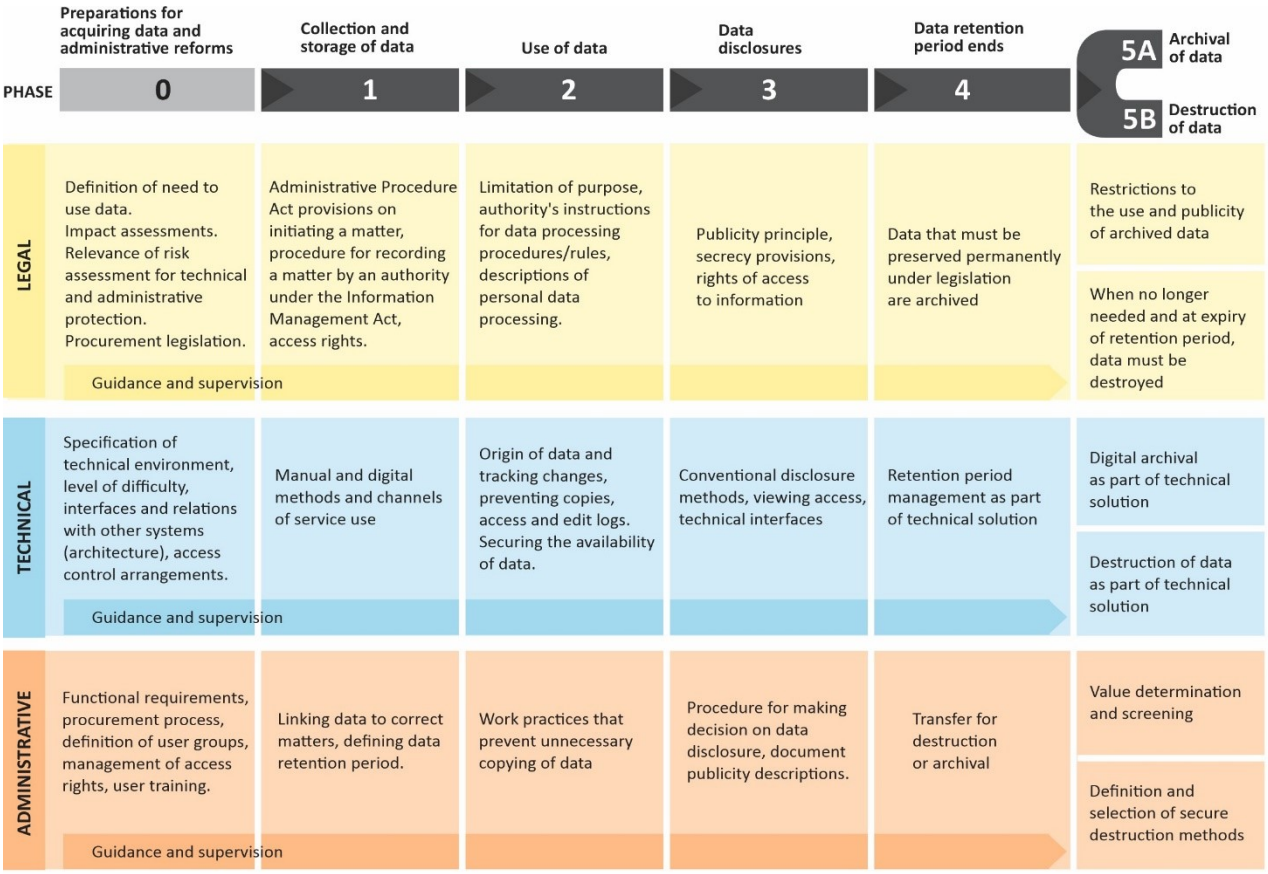

Figure 15. Legal, administrative and technical perspectives on data lifecycle**.**

Openness and secrecy of data

The **Act on the Openness of Government Activities** contains provisions on the publicity and secrecy of data. The basic principle of this Act is the publicity of information and the authorities' duty to promote openness. Section 24 of the Act on the Openness of Government Activities lays down the categories of documents which are secret and to which access is restricted.

Under section 24, subsection 1, paragraph 30, secret documents include:

- documents on student welfare and exemptions from teaching,
- the test results of students and candidates, and
- school diplomas and other documents containing a verbal assessment of the personal characteristics of the student,
- as well as documents indicating the Matriculation Examination Board's division of moderators among the schools putting forward candidates for the matriculation examination, until one year has passed from the examination round in question.

Under paragraph 32 of this subsection, secret documents also include those containing information on the political convictions or the privately expressed views of a person, or information on a person's lifestyle, participation in voluntary associations or leisure-time activities, family life or other comparable personal circumstances of the person.

The special legislation in the education sector contains some provisions on secret information concerning student welfare and the exchange of information between the school and the home.[68]

Position of data breach victims, protection of data and compensation for damage

Under Article 82 GDPR, any person who has suffered damage as a result of an infringement of the GDPR has the right to receive compensation from the *controller or processor* for the damage suffered. A prerequisite for liability is that 1) damage has been caused to either the data subject or another person; 2) personal data was processed in violation of the GDPR, and 3) there is a causal link between the processing of personal data in violation of the GDPR and the damage. The grounds for liability are determined on the basis of Article 82 GDPR, whereas national law is applied to assessing the compensation amount, usually the Damages Act.[69] For example, this may involve a situation where inadequate protection of the register by the controller has made the data breach possible.

If the damage was caused by a party other than the controller or data processor, compensation can be claimed under the Damages Act. Compensation for pure financial loss that is not related to a personal injury or property damage is paid as laid down in chapter 5, section 1 of the Damages Act when it has been caused by an act punishable by law or by the exercise of public authority, or when there are very weighty reasons for this in other cases. Under chapter 5, section 6 of the Damages Act, compensation for suffering is paid when it has, for example, been caused by an act punishable by law that infringes freedom, peace, honour or private life. If a data breach results in personal injury, compensation will be paid on the basis of negligence as laid down in chapter 5, section 2 of the Damages Act.

Material damage for which compensation is paid includes any loss of earnings caused by a data breach and the costs of obtaining a credit freeze. Examples of non-material damage include mental distress and an acute stress reaction that causes temporary disability. A data breach may sometimes also lead to a mental illness classified as a personal injury, such as depression or a panic disorder. In this case, compensation is paid for medical expenses, loss of earnings, suffering caused by the illness and/or permanent or temporary harm.

The Court of Justice of the European Union has ruled that the fear of possible future misuse of personal data also comprises damage for which compensation is due under Article 82 GDPR, as long as the fear is not entirely hypothetical.[70] In *VB v. Natsionalna agentsia za prihodite*[71], the European Court of Justice found that the GDPR does not distinguish between situations where an infringement causes suffering because the party's personal data has already been misused at the time the claim is presented and where the party fears such misuse in future. The wording of the Regulation does not preclude the possibility that the term 'non-material damage' comprises the fear of third parties misusing personal data as a result of an infringement of the Regulation. However, the injured party must demonstrate the negative consequences of the fear. Significant suffering may be caused to a victim of a data breach because

[68] Such provisions are found, among other things, in section 40 of the Basic Education Act (628/1998), section 32 of the Act on General Upper Secondary Education (629/1998), and section 109 of the Act on Vocational Education and Training (531/2017).
[69] 412/1974.
[70] For example, Österreichische Post, C-300/21 and GP v. juris GmbH, C-741/21.
[71] C-340/21.

they fear that the data will be disclosed later in some unexpected context, even publicly on a website or similar.

A special feature of damage caused by a data breach is that compensation cannot restore the situation preceding the event which caused the damage, as later misuse of the data is possible.

Under the Damages Act, the State Treasury may pay compensation for expenses incurred from personal injuries and for pain and suffering as well as temporary and permanent harm. Compensation for suffering is only paid from State funds in certain serious cases, which is why it may not be granted on the basis of a data breach or the disclosure of information that violates private life. Compensation for suffering may be granted on the basis of extortion or attempted extortion. In general, the compensation protection laid down in the Criminal Damages Act is more limited than the right to compensation laid down in the Damages Act, but it provides the victim with certain minimum security that is useful if the perpetrator is insolvent.

In addition to the risk of legal costs associated with criminal and civil proceedings, consideration must also be given to the fact that the proceedings and the documents related to them are public as a rule. Under the Act on the Publicity of Proceedings in General Courts[72], the identity of the injured party may be kept secret in a criminal case that concerns a particularly sensitive aspect of the injured party's private life, and a document containing sensitive information relating to private life or health may be secret. Information may nevertheless be leaked, or all information deemed as secret by a party is not ordered to be kept secret. For this reason, fear of additional publicity may in some cases lead to the victim of a data breach not wishing to demand punishment or claim damages to which they would be entitled.

A personal identity code is a means of identifying a person intended to be permanent. Victims of data breaches often fear that their personal identity codes are used to commit identity theft or fraud, for example. This fear is understandable, even if the personal identity code on its own should only be used as a tool for identifying a person, not as a means of identification on its own – just because a person gives a personal identity code, this does not guarantee that they are the person the personal identity code refers to.

Under the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency[73], a personal identity code can only be changed on strict conditions, which are met if

- the code indicates an incorrect date of birth or gender
- the person confirms that they have changed their gender
- someone has repeatedly misused a person’s personal identity code and has caused major financial or other damage, or
- there is an obvious and permanent threat to a person's health or safety.

After the data breach targeting Vastaamo psychotherapy service (2020), the need to amend the regulation on changing personal identity codes was examined, as personal identity codes could not be changed proactively to protect individuals following security violations or data breaches. However, the conclusion was that there was no cause to relax the preconditions for changing personal identity codes. Persons would incur many kinds of costs and inconvenience

[72] 370/2007.
[73] 661/2009.

from changing their personal identity codes due to the need to change and update documents, customer data and registers.

The misuse of personal identity codes as a means of identification can, for example, be prevented by increasing different parties' awareness of the fact that a personal identity code should not be used alone as a means of identification, and by directing actors to use strong authentication, such as a mobile certificate or online banking credentials. Section 29 of the Data Protection Act contains the following provision on the use of personal identity codes in identification: "The personal identity code alone or a combination of the personal identity code and the name of a data subject must not be used for the purpose of establishing the identity of the data subject based on information given or submitted by the data subject or documents presented by the data subject (*establishment of identity*).

Obligation to provide information and the authorities' obligations to inform victims of a data breach

Under Article 34 GDPR, the controller is obliged to communicate the data breach to the data subject if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication must primarily be made in person and without undue delay.

The communication must clearly describe the data the breach concerns. It must additionally provide information about a contact point where more information can be obtained and describe the likely consequences of the breach. The controller must also describe the measures taken to mitigate its possible adverse effects. The purpose of the information obligation is to ensure that victims of an infringement receive the necessary information to protect their personal data and to take appropriate measures.

In situations where reaching the data subjects would involve disproportionate effort, the information may also be provided as a public communication. Even in this case, the communication must be equally effective, comprehensive and accessible as in the case of a personal communication.[74]

However, the authority's obligation to provide information is not limited to the obligation to communicate laid down in the General Data Protection Regulation. The obligation to provide information must be understood as a broader duty associated with the obligation to safeguard fundamental rights laid down in section 22, subsection 1 of the Constitution. This duty includes the authority's obligation to provide information on its own initiative about matters that are significant or have a broad impact.[75] Among other things, the Chancellor of Justice assessed the fulfilment of this obligation in the context of the procedure for introducing emergency powers at the time of the COVID-19 pandemic. The Chancellor of Justice drew attention to the fact that, especially in exceptional crisis situations, clear and informative communication is essential and that the authorities have a special duty to ensure that citizens have access to information.

The importance of communication is emphasised by the fact that, in a situation that has arisen rapidly, official bulletins may be the only source of information for citizens. In this case, using appropriate and legally precise wordings in communication is essential.[76]

---

[74] Article 34(1)(c) GDPR.
[75] Government proposal for the Constitution of Finland 309/1993 vp, p. 58.
[76] Office of the Chancellor of Justice/740/70/2021 and Office of the Chancellor of Justice/61/10/2020.

The duty to provide information is laid down in section 20, subsection 2 of the Act on the Openness of Government Activities[77], under which the authorities must publicise their activities and services, as well as the rights and obligations of private individuals and corporations in matters falling within their field of competence. The requirement of proper language laid down in section 9 of the Administrative Procedure Act, according to which an authority must use appropriate and comprehensible language, is also associated with the duty to provide information. Section 23 of the Language Act[78] further safeguards linguistic rights in the authorities' communication.

Penal provisions

Chapter 38 of the **Criminal Code** contains the definitions of such offences as interference with an information system (section 7a) and aggravated interference with an information system (section 7b), unlawful access to an information system (section 8) and aggravated unlawful access to an information system (section 8a), offence involving a protection decoding system (section 8b) as well as data protection offence (section 9). The prosecutor shall not bring charges for interference with an information system, unlawful access to an information system or an offence involving a protection decoding system, unless the injured party reports the offence for prosecution or unless the perpetrator committed the offence while in the service of a public postal or telecommunications institution or unless a very important public interest requires that charges be brought (section 10, subsection 3). The prosecutor shall hear the Data Protection Ombudsman before bringing charges for unlawful access to an information system, aggravated unlawful access to an information system, or a data protection offence. When considering such a case, the court shall give the Data Protection Ombudsman an opportunity to be heard (section 10, subsection 4). A legal person may also be liable for punishment with regard to unlawful access to an information system, aggravated unlawful access to an information system, interference with an information system, and aggravated interference with an information system.

The legislation does not stipulate the authority to take command of **cooperation between authorities** in cases of data breaches or cyber security incidents in the same way as in ordinary accidents or offences, in which the rescue or police authorities typically assume overall command. The authorities' responsibilities relating to cyber security and investigating data breaches and threats have been decentralised to different authorities in Finland. Each authority has its own role in investigating incidents in the cyber environment.

In the aftermath of the data breach targeted at Vastaamo, the **Government** adopted on 10 June 2021 a resolution on improving information security and data protection in critical sectors of society. Vastaamo's patient information system was hacked in 2018–2019, and the infringement became public on 21 October 2020 as the perpetrator began to blackmail first the company and, after failing in this attempt, Vastaamo's clients directly.

Personal and health data of an estimated 33,000 psychotherapy clients were stolen in the data breach. The resolution is based on a memorandum of a cross-administrative working group led by the Ministry of Transport and Communications, and it was drawn up during the term of Prime Minister Marin's Government.[79] The resolution defines 37 society level measures to improve data protection and information security as well as to prevent and investigate data

[77] 621/1999.
[78] 423/2003.
[79] Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (Government resolution on improving information security and data protection in critical sectors of society). 1 March 2025 https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82

breaches in critical sectors of society. Around one third of these measures are deemed to include legislative amendments.

The Ministry of Transport and Communications is responsible for promoting and monitoring the fulfilment of the resolution. While the resolution does not clearly define what the critical sectors of society are, the section on implementing measures suggests that they comprise those referred to in the NIS Directive. Education is not one of them.

Key development areas listed in the resolution include improving cooperation, exchanges of information and provision of executive assistance between the authorities, making the information security survey service (Hyöky) and data breach detection service (Havaro) available for all critical sectors, laying down statutory information security requirements applicable to all sectors, obligation to conduct regular information security audits of critical functions, and establishing a service for dealing with and communicating about data protection violations.

In the preparation phase of the resolution, the City Office of Helsinki issued a statement on 7 April 2021 stating that "large organisations, including the largest cities, are able to acquire sufficient expertise in all necessary areas of digital security, such as data protection and cyber security. It is vital that the information security survey service provided by the National Cyber Security Centre is tapped for analysing the level of data protection and information security in the 15 largest municipalities of Finland."

Government resolutions are policy documents that have no direct legal steering effect. However, they describe issues that have been identified as requiring action by the Government. Government resolutions are specific to each government term. As it takes over, a new government usually makes a separate decision on the resolutions it commits to in its work. Prime Minister Orpo's Government made this decision on 21 March 2024.[80] The resolution aimed at improving data protection and information security was also selected as a document that steers the policies of Prime Minister Orpo's Government.

In this context, it has been found that the steering effect of resolutions is undermined by their large number, inconsistent drafting methods and possible disconnection from Government Programme entries.

The task of monitoring the resolution's fulfilment was assigned to the Ministry of Transport and Communications, which has compiled summaries for the ministerial group in charge of follow-up based on reports submitted by the responsible actors.

The legislative measures contained in the resolution have progressed slowly, or the regulatory solutions have changed since the resolution was drawn up. The Act on Cyber Security, which entered into force on 8 April 2025, brought about significant changes to regulation in this field. Such factors as the national implementation of the Network and Information Security Directive NIS2 as part of implementing the Act on Cyber Security have contributed to regulatory solutions and the content of provisions.

The proposal contained in the resolution, according to which cooperation between the authorities in data breach cases be intensified on the same principles that are followed in other serious accidents or incidents, does not loom large in the pending legislative projects.

---

[80] Prime Minister's Office: Erillisten valtioneuvoston yleisistunnossa päätettyjen ohjausasiakirjojen voimassaolosta päättäminen (Decision on the validity of separate policy documents adopted at Government plenary). 26 February 2025 https://valtioneuvosto.fi/paatokset/paatos?decisionId=1079

The Government proposal on developing this measure expired at the end of the electoral term on 4 April 2023.[81]

The **Information Management Board** has issued six recommendations on improving information security in public administration. Several other recommendations also contain information security angles. A recommendation on minimum information security requirements was issued on 11 March 2024. This comprehensive recommendation sets out the grounds regarding minimum information security requirements under the Information Management Act for the public administration. Recommendations and best practices relating to information security are also shared by several other actors, which is why there is no coherent picture of recommended solutions.

A recommendation and criteria to support the assessment of information security in public administration were issued on 12 June 2023. This recommendation has been coordinated with the information security audit tool for authorities (Katakri) and security assessment criteria for cloud services (Pitukri).

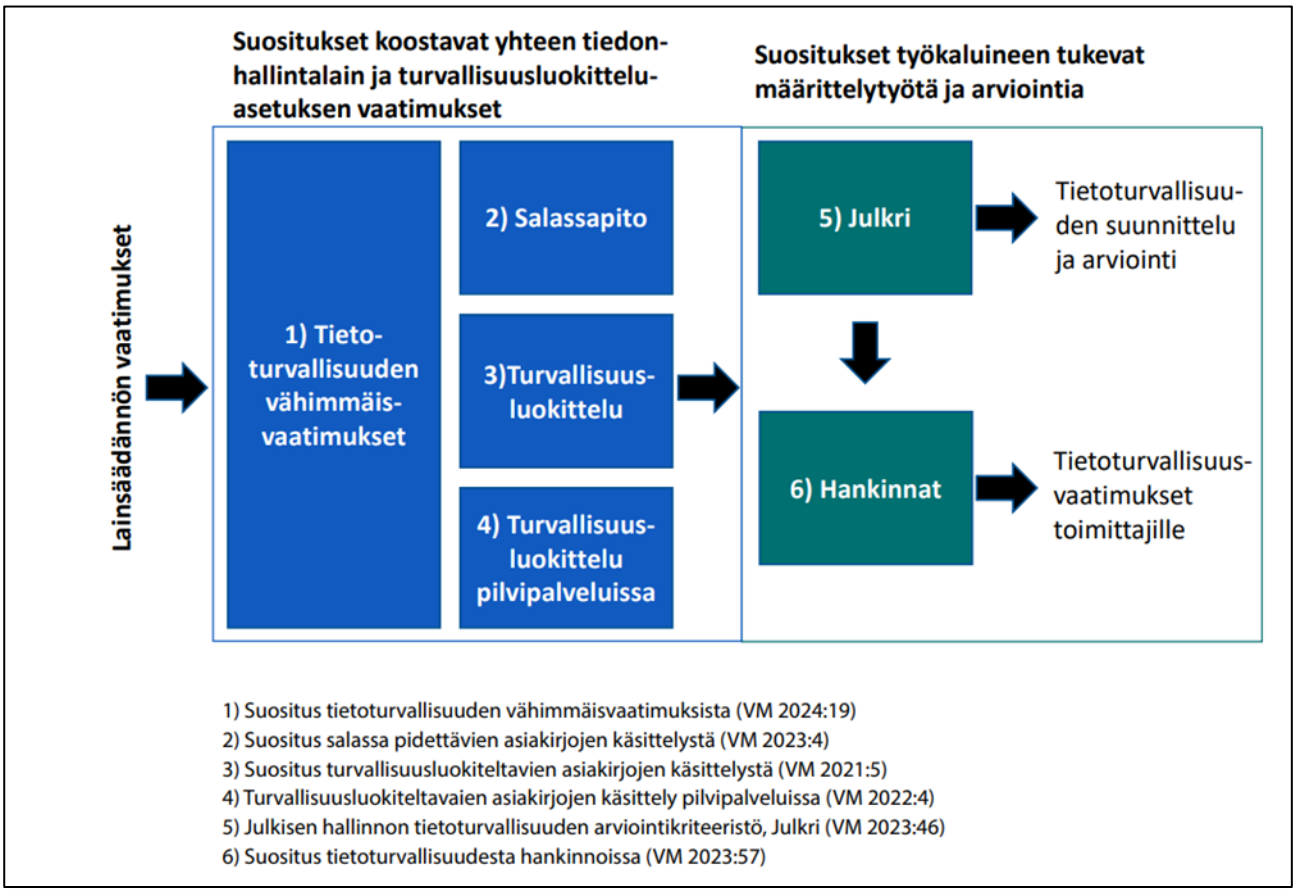

Figure 16. Information Management Board's recommendations on information security (FIGURE: Ministry of Finance 2024)[82]

[81] HE 243/2022. 25 February 2025 https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_243+2022.aspx

82 Suositus tietoturvallisuuden vähimmäisvaatimuksista, p. 10 (Recommendation on minimum requirements for information security). 26 February 2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165487/VM_2024_19.pdf

The Information Management Board has published a recommendation on an information management model to clarify the Information Management Act provisions on the information management model's content.

According to this recommendation, the information management model is a tool that helps the information management entity understand and manage its operating environment and ensure that they meet the information management requirements. The information presented in the information management model lays the foundation for producing the description of the publicity of documents for the customers of an information management entity referred to in section 28 of the Information Management Act.

The recommendation notes that the information management model can provide basic information on the current state of the organisation's information management and its solutions. When the information management model is combined or linked to separate information management control methods of the entity (incl. records creation, information management, quality management), it can also be used to manage the lifecycle of data. The retention periods of the information pool datasets described in the information management model and information on the archival and destruction of data add up to an overview of the lifecycle of the data to be managed in the information management entity. Similarly, metadata that directs the processing of data can be linked to the operating processes presented in the information management model at different process stages.

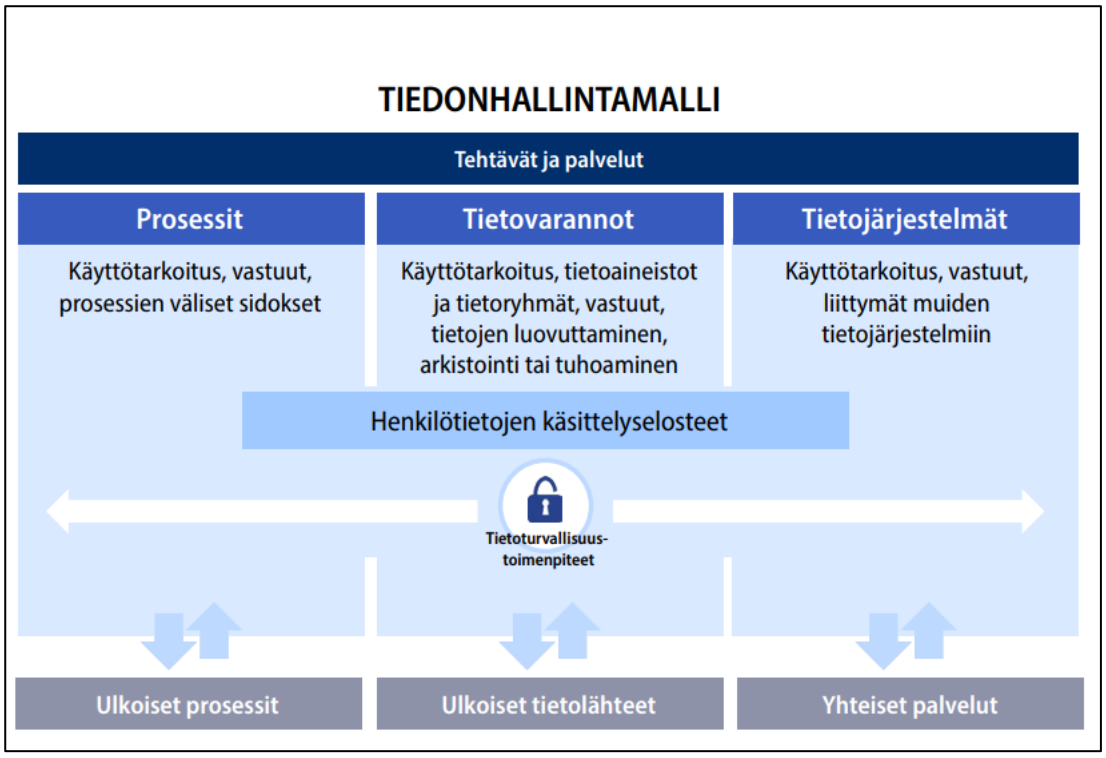

Figure 17. Content of the information management model.[83] (Figure: Ministry of Finance 2024)

The Information Management Board has published a recommendation on information management in connection with service provision. It concerns the authority's datasets that are not

[83] Suositus tiedonhallintamallista, p. 10 (Recommendation on an information management model). 26 February 2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165497/VM_2024_22.pdf

included in the actual processing of a matter. The recommendation supports the fulfilment of the obligation laid down in section 27 of the Information Management Act. It describes the means of carrying out actions related to data identification and lifecycle management.[84]

The decisions of **the Data Protection Ombudsman and other administrators of justice** are published in Finlex database. The decisions comprise case-law, and the legal principles it contains can be used to resolve questions related to data protection.

As part of performing their task, the Data Protection Ombudsman supports compliance with data protection obligations by publishing different guides on key data protection issues. For example, a guide on exchanging information between the home and the school has been prepared for the field of education.[85] Many Office of the Data Protection Ombudsman guides were drawn up before the GDPR entered into force, and they have not been updated to correspond with the Regulation. This undermines their usefulness.

Most guides on data protection in education are publications of the Finnish National Agency for Education. These guides were prepared together with the Data Protection Ombudsman.

In 2021, the Deputy Data Protection Ombudsman submitted an initiative on the processing of personal data in applications used in education to the Finnish National Agency for Education.[86] However, no national guidelines have been completed on the matter.

Finland's Cyber Security Strategy[87] for 2024–2035 was published in October 2024. It has been updated to correspond to the changing operating environment and to bolster the status of cyber security as part of comprehensive security. The strategy has four key pillars:

1. Competence, technology and RDI: Aims to strengthen cyber security competence at all levels of society, promote an innovative cyber ecosystem and use new technologies, including AI and quantum technology.
2. Preparedness: Stresses proactive action to combat and respond to cyber threats, especially to protect critical infrastructure and safeguard the functioning of society.
3. Cooperation: Emphasises the importance of national and international cooperation, including close cooperation with the EU and NATO, as well as public-private partnership in the fight against cyber threats.
4. Response and countermeasures: Develops capabilities for rapid response to cyber attacks, including strengthening cyber defence capabilities and combating cybercrime.

The goal of the strategy is that by 2035, Finland is a pioneer in cyber security where the digital environment is safe and reliable for all users. The strategy will be updated every five years. Its implementation plan is regularly monitored and evaluated.

---

[84] Suositus viranomaisten asiakirjojen metatiedoista palveluja tuotettaessa (Recommendation on the metadata of official documents in service provision) 16 March 2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164194/VM_2022_42.pdf?sequence=1&isAllowed=y

[85] Office of the Data Protection Ombudsman: Oppilaiden henkilötietojen käsittely kodin ja koulun yhteistyössä (Processing of students' personal data as part of cooperation between the home and the school). 26 February 2025 https://tietosuoja.fi/documents/6927448/10594424/Oppilaan+henkil%C3%B6tietojen+k%C3%A4sittely+kodin+ja+koulun+v%C3%A4lisess%C3%A4+yhteisty%C3%B6ss%C3%A4/5169bbf4-c5de-d073-c247-a10a462ca5fb/Oppilaan+henkil%C3%B6tietojen+k%C3%A4sittely+kodin+ja+koulun+v%C3%A4lisess%C3%A4+yhteisty%C3%B6ss%C3%A4.pdf

[86] Office of the Data Protection Ombudsman: Apulaistietosuojavaltuutettu on tehnyt Opetushallitukselle aloitteen opetuksessa käytettävien sovellusten henkilötietojen käsittelystä (The Deputy Data Protection Ombudsman submits an initiative on the processing of personal data in applications used in education to the Finnish National Agency for Education). 26 February 2025 https://tietosuoja.fi/-/apulaistietosuojavaltuutettu-on-tehnyt-opetushallitukselle-aloitteen-opetuksessa-kaytettavien-sovellusten-henkilotietojen-kasittelysta

[87] Finland's Cyber Security Strategy 2024–2035. 26 February 2025 https://julkaisut.valtioneuvosto.fi/handle/10024/165860

The Cyber Security Strategy implementation plan was published on 4 December 2024.[88] It consists of 44 development measures under the four pillars of the strategy, for each of which a target, schedule and funding, impact assessment and analysis as well as organisation(s) and actor(s) responsible for their implementation has been determined.

The statutory duties of the **Digital and Population Services Data Agency** include producing expert services[89] aiming to develop information management and information security procedures for the Information Management Board. A key task is participating in the work of the Board's divisions and in the drafting of recommendations as well as supporting the Board in performing its tasks, for example by participating in the organisation of various events.

In addition, the agency is responsible for the activities of the Finnish Public Sector Digital Security Management Board (VAHTI)[90] and its working groups on developing risk management, continuity, preparedness and readiness, cyber and information security and data protection.

The aim of VAHTI Management Board and working groups is to support and coordinate the development of digital security and cooperation in public administration. They strive to improve the observation capacity and capabilities of digital security, respond to different threats and share up-to-date situational awareness in cooperation with other authorities. They also promote the safe deployment of new technologies in public administration and support cost-effective development in the area of cyber and digital security.

Key tasks of VAHTI Management Board and working groups include:

- Building and reinforcing cooperation networks on developing the public administration's service provision and security in different areas of digital security.
- Monitoring the development of cyber threats and digital security and promoting the sharing of current threat information with public administration actors in cooperation with other authorities.
- Publishing good practices, support materials and other documents and organising seminars and events aiming to promote digital security in public administration.
- Supporting the development of competence, awareness, attitudes and culture relating to digital security in public administration organisations.
- Producing an up-to-date overview and reports on the state of cyber and digital security in public administration and its development needs.

In 2019–2023, the Digital and Population Data Services Agency carried out JUDO, a project funded by the Ministry of Finance, which developed various digital security services. The digital security overview service for public administration[91] enables organisations to compare the level of their administrative digital security with that of other actors. A course and game titled Digitally secure life[92] offer free training for personnel and experts. The app is available for iOS and Android devices.

---

[88] Suomen kyberturvallisuusstrategian toimeenpanosuunnitelma (Finnish Cyber Security Strategy implementation plan). 28 February 2025 https://api.hankeikkuna.fi/asiakirjat/b9b35c4c-2719-4cfb-89fa-4388c855e2f0/c4785613-4037-43b5-b1cc-22d9b82c0d69/KIRJE_20241204070347.PDF

[89] Asiantuntijapalvelut tiedonhallintalautakunta (Expert services for the Information Management Board). 2 March 2025 https://dvv.fi/asiantuntijapalvelut-tiedonhallintalautakunnalle

[90] Digital and Population Data Services Agency, VAHTI. 26 February 2025 https://dvv.fi/en/vahti-network

[91] Digiturvan kokonaiskuvapalvelu (digital security overview service). 26 February 2025 https://www.suomi.fi/palvelut/digiturvan-kokonaiskuvapalvelu-digi-ja-vaestotietovirasto/1b38df61-ca48-41b4-a238-da5ab1baaf27

[92] Digitally secure life training module. 26 February 2025 https://dvv.fi/en/digitally-secure-life

Digital security exercises (Taisto exercises) have been organised annually since 2018.[93] Over seven years, more than 2,200 teams have participated in these half-day or full-day desktop exercises. Most of these teams have been from public administration organisations and comprised more than 14,000 management representatives or experts.

In 2024, the Digital and Population Data Services Agency launched the Databank of digital security service[94] as part of the new Suomi.fi Service Developers platform. The Databank contains key materials on digital security, including legislative and other obligations and existing public support materials. A guide to digital risk management has also been published as part of this service.

Instructions for victims of data breaches and other support services

The data breach targeting Vastaamo showed how important a role different guidelines and other support services play for persons who have been affected by a data breach, their loved ones and the organisation. In the five years that have passed since that event, the situation has improved significantly and guidelines have been harmonised. An increasing number of organisations now offer free support services. Additionally, commercial operators offer fee-based information security services to citizens who use internet connections and smart devices.

The **Digital and Population Data Services Agency** has produced guides for victims of a data breach. The guide titled "*My personal data has been stolen or leaked*"[95] at Suomi.fi offers instructions and advice for persons whose personal data have fallen into the wrong hands as a result of a data breach, data leak or identity theft. The guide helps to identify signs of misuse, prevent malicious use of data, put the necessary bans in place and deal with the aftermath of the situation. The website of the guide attracted a total of 138,000 visitors in May 2024, 25,000 in June, and 67,000 in the last six months of 2024. The guide was updated after the information security violations that occurred in 2024 and with regard to new means of protection.

The guide titled *"Data has been stolen or leaked from my organisation*"[96] at Suomi.fi provides instructions for organisations that have been targeted by a data breach or data leak. It tells organisations what to do in an acute situation, provides advice for preventing further damage, and urges organisations to report the incident to the authorities. The guide also discusses follow-up actions, such as improving information security and updating processes. The website attracted around 7,500 visitors in 2024.

The guide titled "*Preparing for incidents and crises*"[97] at Suomi.fi offers information and instructions on how to prepare for different incidents and crises, including power cuts, storms and disasters. This website attracted 950,000 visitors between November and December.

The **National Cyber Security Centre** has collected on its website instructions and guides on information security skills[98] for private individuals and workplaces as well as practical advice

[93] Taisto-harjoitus on mahdollisuus testata ja kehittää organisaationne digiturvaa (Taisto exercise is an opportunity to test and develop your organisation's digital security). 26 February 2025 https://www.dvv.fi/taisto

[94] Suomi.fi Service Developers: Databank of digital security. 26.2.2025 https://kehittajille.suomi.fi/services/digital-security

[95] Suomi.fi: My personal data has been stolen or leaked. 26 February 2025 https://www.suomi.fi/guides/data-leak

[96] Suomi.fi: Data has been stolen or leaked from my organisation. 26 February 2025 https://www.suomi.fi/guides/data-breach

[97] Suomi.fi: Preparing for incidents and crises. 26 February 2025 https://www.suomi.fi/guides/preparedness

[98] National Cyber Security Centre: Instructions and manuals for private individuals. 26 February 2025 https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/instructions-and-manuals-private-individuals

for victims of identity theft.[99] The website explains what identity theft is and how criminals can misuse personal data. It provides advice on protecting yourself from financial damage, reporting an offence, putting a voluntary credit freeze in place and protecting your account number. It also provides instructions for preventing the misuse of data and finding help in a crisis situation.

After the data breach targeting the City of Helsinki, the **Consumers' Union of Finland** published an article providing instructions for victims of a data breach.[100] It discusses leaked data, including personal data and address information, usernames and email addresses as well as provides advice, which includes monitoring your emails and banking transactions for unusual events. It additionally recommends that consumers change their passwords and use strong, unique passwords in different services. The article also explains what to do if your data are misused.

Victim Support Finland has published advice for victims of a data breach or data leak on its website.[101] The website stresses the importance of following instructions set by authorities as well as putting the necessary bans in place to prevent the fraudulent use of personal data. Victim Support Finland also provides counselling. Its services are free.

Mieli Mental Health Finland[102] offers a number of services to citizens, especially in support of mental health. Victims of a data breach can, for example, call the association's Crisis Helpline or use the support provided by Mieli Crisis Centres.

Sekasin-chat[103] is a national discussion platform for young people aged from 12 to 29 where they can talk confidentially about things that are troubling them. Sekasin Kollektiivi is a consortium coordinated by MIELI Mental Health Finland, the Finnish Red Cross, the Finnish Settlement Movement and SOS Children's Village that works to promote the mental wellbeing of young people and to help them in crises.

KyberVPK Community Cyber Response Force[104] is a Finnish collective of hackers set up to help producers of critical functions combat and recover from attacks. Depending on the needs of the organisation requesting assistance, it can help prevent information security problems, test the security of an environment, solve information security incidents together or, for example, support secure deployment of systems. This voluntary work and free assistance have been provided for the social and health care system, municipalities, educational institutions and other organisations or companies providing critical services and functions.

2.10 Other reports

Elisa Santa Monica's data breach investigation report: The City of Helsinki concluded a contract with Elisa Santa Monica on providing assistance in investigating the data breach on 2 May 2024. As part of this assignment, it mapped the attacker's actions in the intranet and assisted the City of Helsinki in combating the attack. The assignment was extended on 7 May 2024 to cover a full investigation of the information security incident and provision of continuous support for KASKO's information security monitoring. On 7 October 2024, the company

[99] National Cyber Security Centre: Advice for victims of identity theft or data breaches. 26 February 2025 https://www.kyberturvallisuuskeskus.fi/en/news/advice-victims-identity-theft-or-data-breaches

[100] Consumers' Union of Finland: Ohjeita tietomurron kohteeksi joutuneille (Instructions for victims of a data breach). 26 February 2025 https://www.kuluttajaliitto.fi/materiaalit/ohjeita-tietomurron-kohteeksi-joutuneille/

[101] Victim Support Finland: Data breach – Advice to victims of a data breach or data leakage. 26 February 2026 https://www.riku.fi/en/what-to-do-if-your-personal-data-has-been-leaked-online/

[102] Mieli Mental Health Finland. 26 February 2025 https://mieli.fi/en/

[103] Sekasin-chat. 26 February 2025 https://sekasin.fi/

[104] KyberVPK. 26 February 2025 https://kybervpk.fi/en/

produced an extensive investigation report including appendices, in which cyber forensics of network devices conducted by external information security companies and log reports on firewalls and servers were also used.

While the general comment of the **UN Committee on the Rights of the Child**[105] does not deal directly with information security and data protection, the spirit and objectives of the Convention stress the child's right to privacy and safety, which also includes data protection and information security.

The **Office of the Data Protection Ombudsman**[106] has compiled information on children's data protection rights. The Data Protection Ombudsman stresses that every child and young person has the right to data protection. Personal data include a name, address, birthday, telephone number, photos and videos, and information on visits to a doctor. Children also have the right to know where and why their data are processed, and the right to delete or change their data. The Office of the Data Protection Ombudsman ensures that the best interests of the child are taken into account in the processing of personal data.

The **National Child Strategy**[107] highlights children's right to protection and privacy in digital services. This perspective is part of the broader objective of creating a child-friendly and family-friendly society in which children's rights are realised in all areas of life.

The **Central Union for Child Welfare** has released an online publication on viewpoints concerning children's rights and data protection in digital environments[108], which discusses children's rights and data protection on the Internet. Its key message is that the special needs and rights of children must be addressed in the processing of personal data. While children have the same data protection rights as adults, they need special protection, such as the consent of the guardian if under the age of 16. This is the age limit laid down in Article 8 GDPR, from which a Member State can derogate in their legislation, however so that the minimum age limit is 13 years. Finland has made use of this margin of appreciation. Under section 5 of the Data Protection Act (1050/2018), the age limit applied to offering information society services to a child is (at least) 13 years. It also stresses that children must be provided with clear and understandable information on the processing of their personal data.

The **City of Helsinki's internal control** produced a report on the data breach commissioned by the City Manager. This report was completed on 15 August 2024 and complemented with an additional report on 25 November 2024. Among other things, the summary notes that responsibility for the VPN router was left with KASKO as the functions changed, and its maintenance was neglected. No systematic configuration management was in use, and the replacement of the VPN device with an alternative service did not make rapid headway. The transition to centralised data centres had not been conceived as a project at KASKO, and the change was mainly carried out as expert work in addition to other tasks. The change was not considered urgent, and there was no active monitoring of firewall alerts. There was a delay in responding to the data breach. Alerts of atypical observations were triggered as much as five days before the data breach was detected and responded to.

---

[105] United Nations (2001) Convention on the Rights of the Child. 26 February 2025 https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/CRC_General_Comment_1_en.pdf

[106] Office of the Data Protection Ombudsman. Children's data protection rights. 28 January 2025 https://tietosuoja.fi/en/children-s-data-protection

[107] National Child Strategy. 26 February 2025 https://childstrategy.fi/

[108] Central Union for Child Welfare (2019): Lapsi verkossa – Näkökulmia lasten oikeuksiin ja tietosuojaan digitaalisessa ympäristössä (A child online – Perspectives on children's rights and data protection in a digital environment). 26 February 2025 https://www.lskl.fi/wp-content/uploads/Lapsi-verkossa.pdf

According to the National Cyber Security Centre's annual report, the **number of data breaches and other digital attacks** has either grown slightly (data breach attempts, data leaks) or dropped somewhat (data breaches)[109]. Statistical data produced by Finance Finland[110] shows that scams reported to banks have continued to increase throughout the 2020s.

The data breach targeting the City of Helsinki is the most significant such an incident in Finland so far: it targeted around 300,000 people and including not only basic personal data but, in the case of some persons, also personal identity codes and other sensitive data.

Cybercrime has become an increasingly professional, global business over the past decade. Cyber criminals have established CaaS (Crime-as-a-Service) services that offer all necessary tools and other services with a turnkey approach and 24/7 customer support. A hacker may ask a suitable criminal actor to map potential targets, then search for the necessary vulnerability and get the required foothold, after which the hacker can launch an attack of their choice, for example extortion using the data they have stolen.

Microsoft's annual Digital Defense 2024 report[111] notes that, according to the World Economic Forum, cybercrime caused damages exceeding USD 1,000 billion in 2023. Consumer losses amounted to USD 8.8 billion, representing an increase of 30% from 2022.

See the following table for information on **data breaches or denial-of-service attacks targeting the public administration** in 2018–2024 (Table 2):

Table 2: Data breaches targeting the public administration and other significant actors in 2018–2024.

Organisation	Date	Case
City of Lahti	February 2018	Cryptominer program on Provincia's network.
City of Lahti	June 2019	Malware spread to a thousand workstations, incurring costs of EUR 1 million for investigation and cleanup.
City of Kokemäki	August 2019	Ransomware locked the files. Recovery took a few weeks.
City of Pori	August 2019	Ransomware was detected on time (education network).
Municipality of Siuntio	September 2019	Data breach followed by phishing messages under the name of the municipality.
City of Turku	April 2021	Data breach in the education services' network. Ransomware was detected on time.
Savonia University of Applied Sciences	February 2022	Students' personal data were accessed and published on the dark net following a data breach.

[109] Kyberturvallisuus Suomessa (Cyber security in Finland) 17 March 2025 https://kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kyberturvallisuus-Suomessa.pdf

[110] Volume of digital fraud skyrockets in Finland – Banks blocked more than €44 million's worth of fraud-related payments in 2024. 28 February 2025 https://www.finanssiala.fi/en/news/volume-of-fraud-skyrockets-in-finland-banks-blocked-more-than-e44-millions-worth-of-fraud-related-payments-in-2024/

[111] Microsoft Digital Defense Report 2024 28 February 2025 https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Keuda Group, Vocational Education and Training	November 2022	A Lockbit extortion ground the IT environment of Keuda Group to a halt for almost a month. Costs EUR 100,000. No ransom was ever demanded, and there was no data leak.
City of Säkylä	December 2022	An external service provider's error resulted in a security gap in the network. The case was not described in detail in public.
Helsinki Region Transport	December 2022	A significant number of denial-of-service attacks, many of which orchestrated by a pro-Russia activist group called NoName. The same group claimed that it had also attacked other public administration organisations in 2022–2024.
Municipality of Rautavaara	October 2023	Ransomware in the administrative network, the attacker had time to encrypt some of the files.
Tietoevry Oyj	January 2024	Akira malware hit Tietoevry's data centre in Sweden and also destroyed backups. Online stores and many Swedish municipalities incurred major losses from the incident.
City of Helsinki	April 2024	Data breach targeting the City of Helsinki's KASKO intranet, giving an unknown attacker access to copying an estimated 750,000 documents.
Finnish Transport and Communications Agency Traficom	May 2024	Misuse in which a third party managed to download data concerning 65,000 vehicle owners or holders. The same method was also used to target the Positive credit register maintained by the Tax Administration. In this case, the software used by a credit institution had been hacked, as a result of which extracts from the credit register were unlawfully requested from the Positive credit register.
Nordea	September 2024	Several highly serious denial-of-service (DoS) attacks targeting Nordea Bank, which significantly hampered the operation of the online bank and the identification service provided by it.
Vincit Oyj	December 2024	Data breach using the home computer belonging to an employee of IT company Vincit that gave the attacker access to the information system of ten customer companies. The attacker stole a large amount of personal data from Valio.

A **report on the information security and data protection standards of the 15 largest municipalities** was produced after Vastaamo data breach to assess national development needs of information security and data protection in central government. This report was part of the Government's resolution on improving information security and data protection in critical sectors of society (later referred to as the Information security resolution)[112]. The validity of the Information security resolution expired on 10 October 2024 by a Government decision.

One of the measures of the resolution (measure 29) was creating more comprehensive situational awareness of the level of information security and data protection in the 15 municipalities with the largest population in Finland and the critical infrastructure operators in their areas. With regard to critical infrastructure, the focus was on social welfare and health

[112] Ministry of Transport and Communications 2021/44.

care as well as energy and water supply operators. The number of organisations identified using the announced criteria was 66, of which 41 participated in the report.

The report was produced by the Ministry of Finance and the National Cyber Security Centre. The Ministry of Finance was responsible for the overall steering of this project.

The National Cyber Security Centre collected data from energy companies and water utilities and mapped the municipalities' attack surfaces as well as participated in guiding the work on the report and planning, commenting on and writing the report. The Digital and Population Data Services Agency supported the Ministry of Finance by collecting data from municipalities and wellbeing services counties as well as participated in planning and writing the report. Two consultancy companies supported the parties responsible for producing the report, one with the data collection and the other with drawing up the report.

The report was classified and intended to support the responsible authorities and the organisations that were the subject of the report in developing their operations. However, the report brings up development proposals that describe the phenomenon at a general level without disclosing secret information.

As some of its key findings, the report states that at the local government level:

- municipalities should be supported in identifying key assets to be protected
- supply chain risk management is inadequate which, among other things, refers to preparedness in incorporated or outsourced services.

At national level:

- attention should be paid to promoting the extensive use of existing methods and reports in developing activities (cyber maturity studies, digital security survey)
- the existing services should be more readily available for municipalities (especially Hyöky service)
- tools and methods for prevention, development and measurement activities should be used and developed in broader cooperation between the authorities
- making the use of the services mandatory under national legislation should be considered.

The report did not look at the education sector, as it is not deemed to be a critical sector of society for the purposes of implementing the Information security resolution. In its statement issued in the preparation phase of the resolution (3 March 2021), the Finnish National Agency for Education proposes that in addition to the sectors listed in the draft decision as focus areas of the report, the information security and data protection standard of the education services in the 15 largest municipalities in Finland should also be examined. The statement further notes that the education sector processes a large volume of data concerning underage children and, to an increasing extent, special categories of personal data (including information on need for special support), which makes ensuring information security and data protection important.

The **Association of Finnish Local and Regional Authorities** has produced various reports and guides aiming to promote cyber security in local government. A report titled *"Nine digital security challenges highlighted by local government management,"* which was published in 2021, sums up municipal management's views of the situation of digital security in the municipalities. The report includes the following observations:

- municipalities lack a digital security operating model that would guide the management and implementation of digital security in local government

- their ability to respond to sudden attacks is inadequate
- competence is too centralised, the content of the theme is often technological and difficult to understand
- digital security requirements often affect negatively smooth work processes and usability.

According to the report, municipalities need more extensive competence in digital security, and it is not possible to centralise all competence to individual municipalities. This is why the support provided by the Association of Finnish Local and Regional Authorities and other partners is important for municipalities.

The Association has also drawn up *"A digital security check list for local government chief executives*" which lists concisely key issues for which responsibility should be assigned as well as the authorities that can provide support in case of problems.[113] One of the issues the check list does not highlight, however, is that the prevention and investigation of an attack on information networks often requires special expertise, which is mainly available from companies providing information security services.

The Association of Finnish Local and Regional Authorities published *a template of administrative regulations*[114] for the municipalities in 2023. The administrative regulations are the internal rules on the management and administration of the municipality required under the Municipalities Act. Chapter 9 of the administrative regulation template addresses the basics of organising responsibilities for information management and information security in the municipality.

Report on the fight against cybercrime is a Ministry of the Interior publication from 2017. It contains proposals for measures concerning, among other things, developing the fight against cybercrime, improving training related to this fight, developing situational awareness activities relating to cybercrime and legislative reforms. The implementation of the measures proposed in the report was no longer actively monitored, which is why the investigation team asked the ministry's Police Department to prepare a summary of progress made with the measures.

The summary prepared by the Police Department shows that key proposals for measures have made headway. Especially cooperation structures and training have been reformed. Among other things, training on digital forensics in Police University College courses has been developed.

Progress has also been made, or is about to be made, in legislation. The proposals for measures concerning legislation had highlighted the pressures that cybercrime creates regarding the obligation to conduct pre-trial investigations. The proposed measure reads as follows:

> *"Together with the Ministry of Justice, the need to amend the provisions on the conduct of pre-trial investigations by the police will be assessed and, if necessary, legislative amendments will be drafted, ensuring that the investigative resources can be allocated appropriately, taking into account the nature of the offences targeting the cyber environment and the position of the injured party."*

---

[113] Association of Finnish Local and Regional Authorities: Digitaalisen turvallisuuden huoneentaulu kuntajohtajalle (Municipal chief executive's digital security check list). 26 February 2025 https://www.kuntaliitto.fi/sites/default/files/media/file/Kuntajohtajan_muistilista_digiturvallisuus_0.pdf

[114] Association of Finnish Local and Regional Authorities: Hallintosääntömalli (template for administrative regulations). 26 February 2025 https://www.kuntaliitto.fi/julkaisut/2023/2239-kunnan-hallintosaantomalli

The Police Department's summary points out that the cases of Vastaamo and WinCapita show that there is no mechanism in Finland to collectively ensure the rights of victims of crime. It challenges the authorities' ability to deal with cases involving a large number of injured parties. The Finnish criminal process and its rules of procedure are not suited to handling large numbers of injured parties and their claims under private law.

Report on the authorities' capacity to act in cyber security matters is a joint project appointed by the Ministry of the Interior and the Ministry of Defence on 15 February 2022 in keeping with the policies of internal security and defence reports and the earlier Government Resolution of 10 June 2021. The purpose of the project is to assess the authorities' capacity to act relating to ensuring national cyber security, combating cybercrime and cyber defence as well as in rapidly developing situations threatening the cyber security of society, taking into account the continuous evolution of the national and international threat environment.[115] The aim of the report was to prepare development proposals that could be used to improve the authorities' capacity to act.

According to this report, in the real world the authorities usually have clear-cut tasks in managing different threat situations, and the responsibilities and cooperation obligations between the authorities have been defined. Regarding the cyber environment, Finnish legislation does not have sufficient provisions on coordination and cooperation between the authorities at different levels, and the legislation does not sufficiently address the special features of the cyber environment in responding to cyber threats and exchanging information.

The tasks of protecting the cyber environment have been divided between several administrative branches, and responsibility for the cyber environment as a whole has not been assigned, nor can it be assigned, to a specific administrative branch. Close cooperation between the administrative branches, at both the strategic and operational levels, is a precondition for responding to threats. By stepping up the cooperation further, it could be ensured that the correct authority takes action at the right time, however without jeopardising the tasks of another authority, and that the best expertise can be relied on in the activities.

The report finds that the authorities do not currently have sufficient capabilities to efficiently prepare for and combat the most serious cyber threats that endanger national cyber security and national defence. To improve these capabilities, needs for development measures have been identified in seven key areas: the strategic intent of cyber security, cooperation and official processes, situational awareness, exchanges of information, influencing and countermeasures, information acquisition and protection of the authorities' networks.

In addition to the need to step up cooperation between authorities, the fact should be addressed that many of the critical functions of society are firmly in the hands of private sector owners, and that there is significant variation in the cyber security capabilities of these operators. The CERT (Computer Emergency Response Team) function of the National Cyber Security Centre assists actors in the initial investigation of data breaches if necessary, but more extensive investigation and further action relies on private sector services and similar.

[115] The Government (2023): Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa (Report on the authorities' capacity to act in cyber security matters). 26 February 2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164793/VN_2023_31.pdf

3 ANALYSIS

To analyse the event, the Accimap[116] method developed further by the Safety Investigation Authority was used. The analysis text is structured based on an Accimap diagram prepared in the course of the investigation, which describes the incident as a chain of events in the bottom part of the diagram. Factors emerging in the background of the chain of events are analysed in the diagram at different levels.

3.1 Analysis of the event

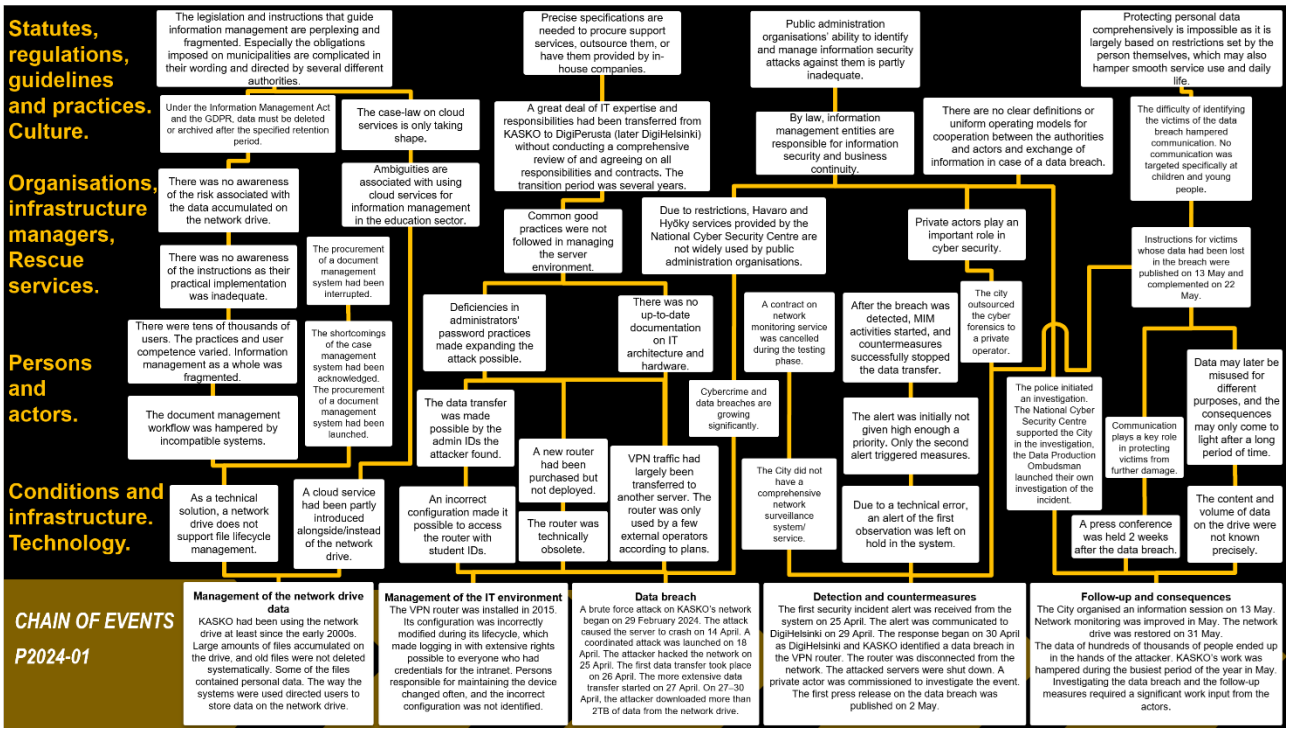

Figure 18. ACCIMAP analysis diagram P2024-01.

3.2 Management of the network drive data

In the early 2000s, the City of Helsinki's Education Division (KASKO) deployed a network drive on which files could be stored quite freely. All KASKO employees could access the drive and, over the years, it had tens of thousands of users. Over time, more than four million files were accumulated on the drive, some of which contained sensitive information belonging to special categories of personal data. The contents of the drive were not examined systematically during these years, nor were old files deleted. While network drives are a technology that has been in wide-spread use for a long time, as a technical solution they do not support systematic information management or the data lifecycle model.

Data that supported work and were associated with preparing decisions had to be stored on the network drive, which was also used by the official case management systems. This was due to the City of Helsinki's multiple information systems, which had not been integrated into a coherent case management system.

---

116 Rasmussen, J. & Svedung, I. (2000) *Proactive Risk Management in a Dynamic Society*. Karlstad, Sweden: Swedish Rescue Services Agency.

The City of Helsinki had provided the personnel with instructions on information management and the use of the IT environment. The instructions were partly fragmented as they were found in the City's various document management systems. The key problem was KASKO personnel's low level of awareness of the instructions which consequently had little or no impact on practical work.

The City of Helsinki had identified shortcomings in its document management systems and launched a public procurement to remedy this issue. However, the Market Court cancelled the contract due to a formal error.

The City of Helsinki had partly switched to using cloud services instead of network drives. However, a large part of KASKO organisation had continued to use the drives. Ambiguities relating to legal preconditions for and restrictions of their use have contributed to slowing down the deployment of cloud services in local government. The case-law is also only taking shape.

Permissions for the network drive had been granted to each individual office and function and backups of the drive had also been provided for, but there was no awareness of the risks arising from the large number of files accumulated on the drive or leaks from it.

A great deal of legislation and guidelines as well as several authorities have a bearing on information management. The legislation is fragmented and found in a number of acts, and perceiving the whole is difficult. Under the Act on Information Management Act in Public Administration and the EU General Data Protection Regulation, stored data must be deleted or archived within the time frame specified by the organisation.

3.3 Management of the IT environment

The data breach targeted a VPN router that was commissioned in 2014. Most of the remote connections to KASKO's network had already been transferred to other VPN routers, which is why the ASA 5515 router targeted by the breach was mainly used by external actors. The device was technically obsolete and its security updates had been neglected. A replacement device had been purchased for the router but not deployed.

The most crucial factor for the success of the data breach was an incorrect configuration, which enabled access to the system with student IDs and granted extensive rights to use the intranet. The investigation could not determine the date on which this setting was made, or the person who made it. The responsibility for maintaining the device had shifted several times and was also unclear at the time of the data breach.

The administrator IDs found by the hacker on the intranet and shortcomings in password practices made it easier for the hacker to hack additional servers. As a whole, good IT practices were not followed in the management of the telecommunications and server environment.

The City of Helsinki's IT services had been reorganised over the past five years. They had been centralised, first to Digitaalinen perusta and later to Digi Helsinki. KASKO as a division had mainly continued to maintain its own IT system. A large number of organisational and personnel changes had occurred in the division, however, as a result of which KASKO's responsibilities for IT maintenance were partly unclear. The local government sector has generally recognised the challenges associated with procuring external services, outsourcing and using in-house companies in the provision of services.

3.4 Data breach

The way for the data breach had been paved by means of a brute force attack carried out in late February and March 2024 as well as by scanning the environment. The VPN router used by KASKO was attacked on 14 April 2024 using a known vulnerability, which caused the router to crash. However, the cause of this was not investigated, even if an investigation would have revealed that the device was still in use and that it had not been updated, as well as the fact that the device log was not functioning because the disk space on the separate log server was full.

The actual data breach was launched on 18 April 2024. The hacker logged into KASKO's intranet via the router on 25 April 2024, at which time the first file download from the intranet took place. The most significant file transfers took place in the period between 27 and 30 April 2024, during which the total amount of data exported was around two terabytes (approximately 750,000 files).

Data breaches have generally been increasing in recent years. The National Cyber Security Centre produces situational awareness for society and organisations through its Havaro and Hyöky services. While the City of Helsinki has been a Hyöky customer since late 2023, the vulnerable router had been excluded from the checks carried out by the service.

The services provided by the National Cyber Security Centre are not widely used by public sector organisations, as the National Cyber Security Centre has not had the resources needed to develop and maintain these services for this target group.

Cybercrime poses a significant threat to the public administration, which collects large amounts of data concerning citizens. This is why public organisations can be attractive targets for hackers. In most cases, data processing in public administration is based on compliance with a legal obligation, which means that the data subjects' possibilities to restrict and control the use of their data are limited. The subordinate position of the customer highlights the public administration's obligation to protect data subjects’ data.

The responsibility of organisation management for information security and data protection is straightforward.

3.5 Detection and countermeasures

The malware detection program issued alerts on 25 April 2024, but KASKO was only informed of them on 29 April 2024. Even then, the critical nature of the alerts was not immediately recognised, which is why the countermeasures were only started on 30 April 2024.

KASKO and DigiHelsinki located the VPN router that was the source of the data breach. It was disconnected from the network, and the other servers that were attacked were shut down. The delay between initial detection and the launch of countermeasures was affected by technical and process-related errors in the service request system and shortcomings in the information flow between actors.

Had comprehensive log management and a security operation center been in use, the attack would probably have already been detected in the preparation phase and the data breach would have failed. Real-time network monitoring would have detected exceptionally large night-time data transfers from the intranet to the Internet. The City of Helsinki was in the process of procuring an extensive network surveillance system, but its procurement had been suspended as the customer had not been satisfied with the results of the commissioning testing.

As the City's own resources and expertise were found to be insufficient, the investigation and management of the data breach were outsourced to an external company. Resources critical for information security are in the hands of private operators, and those available to the authorities are limited. Public sector actors are unable to provide extensive support to actors in data breach cases or other crisis situations related to information security. Cooperation between the authorities in these situations is partly unstructured and does not always support incident management.

The City of Helsinki set up several working groups that met regularly and frequently to manage the crisis. The City started public communications with a media release on 2 May 2024. As the data breach investigation progressed, the original situational awareness of the incident, its consequences and impacts on different target audiences was enhanced due to the additional information.

In data breaches, attention is often focused on the technical details of the incident, such as system vulnerabilities and information security measures. The role of communication is equally critical, however: it has a direct impact on the victims' ability to protect themselves against further damage. Clear, rapid and consistent communication helps to manage the situation, prevent misinformation and ensure that the parties receive the support and instructions they need.

3.6 Follow-up and consequences

A press conference was organised 11 days later on 13 May 2024. At the press conference, guidance was provided, noting that the situation and its scale were still being investigated. The press release of 21 May 2024 stated that the target groups of the data breach had expanded.

In communication (esp. crisis communication), it is not possible to wait for the final results of the investigation, as it is important to provide an early overview of the situation and inform the victims of the data breach about protection measures. While data breach mitigation starts with insufficient information due to incomplete situational awareness, openness builds trust and prevents the creation of an information vacuum and spread of speculations.

The City of Helsinki quickly targeted communication at its employees and students' guardians. To support personal and interactive communication, a helpline was provided for the victims of the data breach and other parties, such as guardians. However, communication was not targeted at different age groups, such as children and young people according to their age level, and it did not address the needs of children and young people (or minority language groups), for example by using clear language, visual content or communication channels used by these groups. For example, minors could be reached comprehensively and effectively in their school classes, as this makes it possible to inform students directly in an age-appropriate way while also giving them an opportunity to ask questions and receive guidance.

On 18 June 2024, the City of Helsinki reported that the data breach targeting the City had not expanded. On 12 July 2024, the City informed the residents that an investigation team appointed by the Government would launch an investigation of the data breach targeting the City of Helsinki. The City of Helsinki next released information on the situation of the data breach on 17 December 2024.

Pursuant to Article 34 GDPR, communication with victims of a data breach must primarily be carried out in person and without undue delay if the breach is likely to pose a high risk to the rights or freedoms of the data subject.

The City of Helsinki quickly targeted internal communication at its employees. The City's employees could be reached quickly through personal messages, as their email addresses were known and they could be informed of the data breach without delay both on the City's intranet and by personal email messages. To support personal and interactive communication, a helpline was provided for the victims of the data breach and other parties.

Reaching out to former and current learners, their guardians and other people who had dealt with the City proved considerably more difficult. Informing all data subjects personally was considered impossible, and it was not attempted. Whereas the General Data Protection Regulation allows the use of a public communication when reaching individuals would require a disproportionate effort, this does not automatically guarantee the effectiveness or coverage of the communication.

Being the victim of a data breach may cause many types of health risks and mental stress, disrupting the person's sense of security. Stolen data can be used for criminal purposes, including identity theft, financial fraud, extortion and scams, as well as to damage a person's reputation even after many years. The impacts of misuse may not be immediately apparent.

Minors may not be able to protect their data, or know how to do it. They may also be unaware of the importance of data protection. They may not know how their data can be used for criminal purposes, and they may not always understand the importance of being protected. Protection measures, such as credit freezes or requests for deletion of data, may additionally be complex from a minor's perspective and require their guardian to take action. They may be equally challenging for those who do not speak Finnish, Swedish or English.

It is important that young people and their guardians are offered clear and accessible instructions on preparing for data breaches and minimising their consequences. Instruction and media education can also help young people understand how their data may be used and how they can protect themselves better.

By the time this report was completed, no indication of the personal data being spread on the dark web or used for identity theft has been detected. Future use of the data cannot be excluded, however.

4 CONCLUSIONS

Conclusions encompass the causes of an accident or a serious incident. Cause means the different factors leading to an occurrence as well as relevant direct and indirect circumstances.

1. Over the years, different types of data were accumulated on the network drive and the removal of unnecessary data and organisation of files, which depended on employees' personal initiative, were neither carried out systematically nor supervised.

   Conclusion: *Building data lifecycle management on measures implemented by the users exposes the organisation to a situation where data processing and information management add up to an unmanageable whole.*

2. While the Act on Information Management in Public Administration is coordinated with the General Data Protection Regulation, together with other statutes applicable to public administration, including the Administrative Procedure Act, Act on the Openness of Government Activities, Archives Act and special legislation, information management as a whole appears difficult to understand, and various acts lay down a number of similar assessment and planning duties.

   Conclusion: *Information management in public administration involves a number of statutes adopted at different times that do not form a clearly coordinated entity. This makes it difficult for those responsible for information management to understand the requirements as a whole and leads to their varying application.*

3. Information management, information security and data protection in public administration are steered by several different authorities which perform their tasks independently, each from their own perspective.

   Conclusion: *As information management is steered by several authorities, the guidance of information management entities is fragmented, and in practice the statutes and instructions are applied to variable degrees. While the authorities provide guidance, there is little supervision of the actors.*

4. Cybercrime is a growing area of criminality that causes significant harm. Public administration is an attractive target for criminals because of the quality and quantity of data it possesses.

   Conclusion: *The public sector's capability to respond to cybercrime threats is currently inadequate, as the methods for detecting attacks and vulnerabilities are not used comprehensively. By identifying and eliminating attacks and vulnerabilities, data breaches can be prevented and the data protected.*

5. An outdated VPN router remained in use even though most of its users had moved on to a new device. No one was clearly responsible for the device, which is why its maintenance was minimal and limited to the mandatory certificate renewal.

   Conclusion: *As technologies and organisations change, some IT hardware is poorly maintained, posing a risk of data breaches.*

6. Inclusive network surveillance could have detected the preparation of the data breach several weeks earlier. Attempts to expand the breach on the intranet triggered alerts but the response was insufficient.

   Conclusion: *A successful data breach is rarely caused by a single error or neglect. Network surveillance is a key part of managing an IT environment securely. Missing*

log data slows down the investigation of damage, hinders cleanup and hampers preparation for future attacks.

7. In the event of a data breach, the responsibility for investigating and preventing the attack lies with the affected organisation. The City launched countermeasures to the data breach with the information security company it hired. Authorities also participated in the response and investigation.

   Conclusion: *The public sector depends on the expertise and availability of private sector actors for investigating and managing data breaches. No operating model for launching cooperation, exchanging information and coordinating measures had been defined.*

8. The City of Helsinki started communicating internally about the data breach immediately, but there was a delay in external communications. The city's employees were quickly reached through personal messages, whereas targeting communication at former and current learners, their guardians and other customers of the City was more difficult.

   Conclusion: *Reaching data breach victims may be challenging. Issuing a public communication is important. It, however, does not solely suffice to ensure that the communication reaches the victims. Proactive communication planning and multi-channel communication are important for protecting the victims of a data breach.*

9. Information targeted at children and young people was inadequate and did not sufficiently address the needs of different ages and special groups, for example by means of age-appropriate communication.

   Conclusion: *Underage data breach victims may not be able to protect their data themselves. This makes targeting communication at children, young people and guardians important, and the difficulties it presents must not be an impediment.*

10. In Finland, citizens can restrict the use and disclosure of their personal data in public information systems. This is based on settings that restrict the use of personal data made by the person themselves which, however, cannot fully prevent the use of the data for criminal purposes.

    Conclusion: *Protecting personal data comprehensively is impossible and largely based on restrictions set by the person themselves, which may also hamper smooth service use and daily life. The victim of a data breach is exposed to a long-term risk of later misuse of their data.*

5 SAFETY RECOMMENDATIONS

5.1 Coordination of information management legislation

The statutes to be complied with in the public administration's information management have been adopted at different times. The key requirements of the GDPR were taken into account when passing the Information Management Act, and the Act can be considered to be aligned with the GDPR. Some of the regulation on information management continues to be found in other statutes. Provisions are contained in special acts and general administrative legislation, including the Archives Act and the Act on the Openness of Government Activities. They have not been comprehensively coordinated from the start till the end of the data lifecycle, and especially the statutes and regulations concerning archiving are old. Technological solutions have also developed rapidly, which increases the need for legislative reviews.

The division of oversight and steering duties between several different authorities is also likely to undermine the consistency of the guiding documents and their application.

The investigation team recommends that

The Ministry of Finance in cooperation with the Ministry of Justice ensure that the legislation on information management in public administration is coordinated and that the structures for monitoring and steering it are clarified. [2025-S4]

Among other things, the statutes impose overlapping planning and assessment obligations on entities, including the use of an information management model, impact assessment and risk assessment. Attention should also be paid to the implementation of legislation, guidance for its application, and support for those applying it in different interpretation issues. Among other things, practical application problems have been caused by implementing information management in services and the use of cloud services in the processing of personal data.

5.2 Developing the detection of information security shortcomings in public administration

Proactively detecting information security shortcomings in public administration is an effective way of preventing the exploitation of vulnerabilities and, consequently, data breaches. The growth of cybercrime requires extensive and multi-layered development of information security measures. This means that it is important to continuously update and improve security practices and use the latest technologies and methods. It is also essential to provide the personnel with training on information security issues and to ensure that all levels of the organisation are aware of potential threats and know how to tackle them. This will help create a comprehensive and efficient security system that protects public administration data and resources.

The investigation team recommends that

The Ministry of Finance in cooperation with the Ministry of Transport and Communications investigate how the detection of information security deficiencies in public administration can be improved nationally and ensure that public actors have sufficient capabilities for detecting and addressing shortcomings in information security. [2025-S5]

The current Hyöky service is not widely used by public administration actors. However, a service for identifying information security gaps is needed that is easy to use and that can be deployed by all public organisations. This will enable overall improvement of information security in public administration.

5.3 Developing communication guidelines for data breaches

Communication is part of preparedness for data breaches. For this, up-to-date communication guidelines are needed. Once a data breach occurs, it is important to communicate quickly, clearly, accessibly and consistently. This reduces uncertainty, prevents the spread of misinformation and ensures that victims receive the support they need. In addition, guidance and support must be provided to those whose data have been compromised. Information on data breaches must be provided on multiple channels as well as be age appropriate, targeted and accessible, ensuring that it reaches the victims of the data breach extensively and comprehensibly. In the absence of clear and consistent communication about the data breach, several risks may arise. Uncertainty increases when parties do not know what has happened and how it affects them, which may cause unnecessary concern and stress.

The investigation team recommends that

The Ministry of Finance in cooperation with the Finnish National Agency for Education ensure that municipalities and cities develop clear and accessible guidelines for communicating about data breaches, enabling victims to protect themselves from the consequences of data breaches and protect their personal data. [2025-S6]

When developing communication, the aim should be at broad-based cooperation, especially with the Ministry of Education and Culture and the National Cyber Security Centre. In practical implementation, it is advisable to use the channels favoured by young people, including social media and instant messaging services, as well as inform guardians through journalistic media, e-mail, letters and official websites. In addition, a school class is an effective way of reaching minors, making it possible to provide guidance and handle questions in an age-appropriate manner.

5.4 Identifying and remedying municipalities' critical information security shortcomings

To ensure information security and prevent data breaches, municipalities must take proactive, immediate and continuous measures to improve risk management related to the processing and storage of data.

Identifying and managing the risks related to the processing and storage of data are key measures for ensuring the reliability of data and information security in public services.

Regular risk analyses help identify and fix potential problems in time.

The investigation team recommends that

The Ministry of Finance in cooperation with the Association of Finnish Local and Regional Authorities support municipalities in identifying and addressing critical information security shortcomings and develop risk management relating to information management and information security. [2025-S7]

Organisations must identify the locations where they have stored personal data. Storage locations used by the organisation, such as network drives, chat services, email and cloud services, should be examined immediately. The information security of remote connections should also be ascertained.

It is advisable to involve the wellbeing services counties and other stakeholders in the development work.

5.5 Actions taken

The **City of Helsinki's action plan** after the data breach was launched by decision of the City Manager. In this context, shortcomings in case management and information security were examined by Division, and corrective measures associated with them were determined. The measures were implemented in an order of priority. The measures addressed the factors that enabled the detected data breach, including information security training for the personnel, practices of using remote connections, data storage locations and defining responsibilities for deleting data. The development programme includes a regular reporting duty to the City Manager in interim reports.[117]

The **City of Helsinki made a contract award decision** on procuring additional information security measures from DigiHelsinki Oy on 12 August 2024. These measures are related to addressing the information security deficiencies detected due to the data breach. The value of the additional procurement was EUR 2.6 million.[118]

The **NIS 2 Directive** is the European Union’s cyber security directive, the aim of which is to strengthen the Union's common and Member States' national level of cyber security, especially in critical sectors. It lays down minimum measures for cybersecurity risk management and notification obligations in significant incidents. The Directive was adopted in November 2022 and had to be transposed into the Member States' national legislation by 17 October 2024. The acts implementing the NIS 2 Directive were submitted to Parliament on 23 May 2024, they were passed by Parliament in March 2025, and they entered into force as from 8 April 2025. Provisions on the new obligations of the public administration under the NIS 2 Directive are laid down in the new chapter 4a of the Act on Information Management in Public Administration. The obligations applicable to other organisations are prescribed in the new Act on Cyber Security. These Acts entered into force on 8 April 2025. Under the Act on

[117] City Manager's action plan (City of Helsinki 3 September 2024).

[118] Procurement, additional information security measures purchased from DigiHelsinki Oy, City Executive Office. 28 February 2025 https://paatokset.hel.fi/fi/asia/hel-2024-011885?paatos=484a470a-21d9-4e44-a0c2-b4ce754116e1

Cyber Security [124/2025], the authority tasked to oversee public administration is the Finnish Transport and Communications Agency. It should also be noted that the municipalities are not within the scope of the Act on Cyber Security, apart from any service that they may provide. The new Act on Cyber Security that entered into force in spring 2025 and amendments to the Information Management Act also impose new obligations on public sector actors. The Finnish Transport and Communications Agency is the authority that oversees public sector actors and, in this new role, will strive to clarify the guidance and supervision structures of the sector.

CER, or the **Critical Entities Resilience Directive**[119] entered into force on 14 December 2022, and the Member States were to transpose its requirements into their national legislation by 17 October 2024. The CER Directive aims to improve the resilience of interdependent services that are critical for the functioning of society and to maintain the economic functions of society. The CER Directive would be implemented by adopting a general act on the protection of critical infrastructure in society and improvement of resilience, which would provide for a national strategy on critical infrastructure and the resilience of critical entities as well as a national risk assessment, general steering and coordination of activities, a commensurate assessment framework for critical entities, and a coherent framework for reinforcing the resilience of critical entities in face of various threats. The Directive introduces new tasks for the coordinating ministry, sectoral ministries and authorities. Pursuant to the Directive, the new task must be identified, and critical entities and supervision tasks must be determined using uniform procedures. The sectoral oversight authorities would be competent to supervise critical entities. Key obligations applicable to the critical entities would relate to risk assessment, resilience plans and ensuring resilience, as well as incident procedures.

The CRA, or **Cyber Resilience Act**[120] (EU) 2024/2847 is a European Union regulation aiming to improve the cyber security of digital devices and software on the EU market by reducing vulnerabilities. The Act sets minimum cybersecurity requirements for all devices and software that can be directly or indirectly connected to another device or network. This includes security cameras, televisions, toys, home routers, firewalls and various software, such as operating systems and browsers.

Manufacturers are responsible for the cyber security of their products throughout their lifecycle. They must ensure that the products are designed, developed and manufactured in compliance with the essential cyber security requirements of the Act. These requirements include safe default settings, automated security updates, prevention of unauthorized access, and confidential processing of data. The manufacturers must also clearly indicate the length of the support period for their products and actively report on exploited vulnerabilities and serious information security incidents to the European Union Agency for Cybersecurity (ENISA) and national CSIRTs.

[119] CER Directive, Government proposal HE 205/2024. 28 February 2025 https://www.finlex.fi/fi/hallituksen-esitykset/2024/205#OT0

[120] Cyber Resilience Act (CRA). 28 February 2025 https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra#76938-0

REFERENCES

The investigation team received written investigation documents and conducted hearings pursuant to the Safety Investigation Act (525/2011). The team contacted 26 organisations. Through hearings and preliminary interviews, information was obtained from around 60 people. The organisations that provided information to the investigation team are:

1. Digital and Population Data Services Agency
2. DigiHelsinki Oy
3. Dustin Finland Oy
4. Elisa Santa Monica Oy
5. Fujitsu Finland Oy
6. City of Helsinki
7. Helsinki Police Department
8. University of Helsinki
9. National Bureau of Investigation
10. Experts by experience
11. Association of Finnish Local and Regional Authorities
12. Office of the Ombudsman for Children
13. Ministry of Transport and Communications
14. Finnish Transport and Communications Agency, National Cyber Security Centre
15. National Defence University
16. Ministry of Education and Culture
17. Finnish National Agency for Education
18. Palo Alto Networks
19. Ministry of the Interior
20. Finnish Security and Intelligence Service
21. Telia Cygate
22. Information Management Board
23. Office of the Data Protection Ombudsman
24. Office of the National Cyber Security Director, Ministry of Transport and Communications
25. Ministry of Finance
26. Victim Support Finland

SUMMARY OF COMMENTS RECEIVED ON THE DRAFT INVESTIGATION REPORT

The draft investigation report was circulated for commenting to the Ministry of Finance, Ministry of Transport and Communications, Ministry of Justice, Ministry of Education and Culture, Ministry of the Interior, Traficom's National Cyber Security Centre, Finnish National Agency for Education, City of Helsinki, Finnish Security and Intelligence Service, National Bureau of Investigation, Helsinki Police Department, Digital and Population Data Services Agency, Office of the Data Protection Ombudsman, Information Management Board, Association of Finnish Local and Regional Authorities, Office of the Ombudsman for Children, Elisa Santa Monica Oy and Telia-Cygate.

Pursuant to the Safety Investigation Act of Finland, comments given by private individuals are not published.

The **Ministry of Finance** notes in its statement that the investigation report describes the data breach targeting the City of Helsinki's Education Division and the reasons that led to it exceptionally well and thoroughly. The Ministry of Finance points out that while the recommendations made in the investigation report focus on legislation and guidelines, the report does not show that the state of the legislation would have actually affected the data breach. The Ministry of Finance proposes that instructions be added to the recommendations included in the investigation report that, when followed, would make it possible to avoid the shortcomings discovered by the report in such areas as service management, supplier management and asset management. The Ministry of Finance would also welcome the conduct of an investigation similar to the one described in this report in all significant data breach cases.

The ministry notes that the investigation report does not relate to the local government sector at large, and by analysing the events in one municipality, no conclusions can be made that are applicable to all municipalities. Regarding the safety recommendations given in the investigation report, the Ministry of Finance highlights the challenges it faces in influencing the conduct and schedules of drafting statutes which other ministries are responsible for. This is why assigning responsibility for coordinating some of the measures primarily on the Ministry of Finance is problematic. The Ministry of Finance further points out that regulation on information management is also contained in special acts falling within other ministries' remits, and these acts are always drafted by the ministry responsible for the regulation in question. The Ministry of Finance points out in its statement that it can promote coordination by various means, including statements and guidelines, but the ultimate responsibility for coordination rests with each ministry that drafts the regulation.

The Ministry of Finance notes that, based on its general duty to oversee the municipalities' operations and finances, it has no right to access information on how an individual municipality has arranged its internal control and risk management and whether these arrangements are adequate, including responsibility for information security and detecting shortcomings. The ministry notes that consequently, forming situational awareness of individual municipalities or creating a system for detecting shortcomings that covers the entire local government sector cannot be a task for the ministries. The Ministry of Finance additionally points out in its statement that in keeping with their autonomous status, the municipalities are themselves responsible for their arrangements relating to information management and information security as well as communication as laid down in the Municipalities Act (410/2015). It also notes that the municipality performs the duties it has taken on by virtue of its autonomy and makes arrangements for performing the tasks separately imposed on it by law.

The Ministry of Finance stresses that detecting and rectifying shortcomings in information security and developing information management and data protection are part of the municipality's internal control and risk management, and the responsibility for them consequently rests with its municipal board. The Ministry of Finance also notes that the ministries cannot be responsible for developing risk management in information management and information security or, for example, ensuring adequate capabilities in all municipalities. This also applies to ensuring adequate communication.

In the Ministry of Finance's view, the municipalities' responsibility for information management arrangements should not be bypassed solely on the grounds that, in terms of overseeing the fulfilment of a safety recommendation, targeting the recommendation at ministries is easier. The Ministry of Finance also points out that currently, no recommendations have been addressed at the municipalities or their auditors. The Ministry of Finance notes that the needs of identifying and rectifying shortcomings in information security may vary from one organisation to another, which is why each organisation is responsible for them. According to the Ministry of Finance, recommendations concerning municipalities could also be needed for the wellbeing services counties.

The **Ministry of Transport and Communications** finds in its statement that the investigation report describes clearly the progress of the situation as well as the events that occurred and the actions that were taken during it. The investigation report elucidates factors that led to the case and its consequences, making it possible for other organisations to benefit from the investigation observations to improve the security of their activities and consequently prevent new incidents.

The Ministry of Transport and Communications also notes that the level of cyber security is also significantly influenced by the resources various organisations allocate to cyber security, in addition to which resources are needed for developing the authorities' activities and services. The investigation report does not bring up the significance of the straitened situation of general government finances for the public administration, in particular, and consequently on the cyber security services provided. The Ministry of Transport and Communications stresses that detecting shortcomings in information security and other services to be provided in order to improve cyber security require continuous resource allocations.

The ministry also notes that the recommendations are currently mainly addressed at the ministries, and to avoid similar incidents and hazards in the future in municipalities, companies and other organisations alike, also targeting recommendations at them should be considered to improve proactive preparedness.

The Finnish Transport and Communications Agency Traficom points out that ensuring the continuity of the services provided by Traficom's Cyber Security Centre and expanding the use of these services, including the Cybermeter and Hyöky, to further target groups as well as safeguarding the activities and continuity of the HAVARO service are also included in Finland's Cyber Security Strategy 2025–2035 and its implementation plan. However, the strategy also notes that additional resources will be needed for these actions.

The Ministry of Transport and Communications points out in its statement that it is important to draw on the experiences gained during the investigation of the data breach that targeted the City of Helsinki and the completed investigation report to support legislative drafting and to act on the relevant Government Programme entry. In legislative drafting, different options for ensuring cyber security should be considered. In the context of conducting safety investigations of serious incidents, it should also be noted that exceptional incidents can already be investigated in the current situation.

The **Ministry of Education and Culture** notes in its statement that the investigation report is well prepared and thorough. The report contains essential and valuable information on the reasons and impacts of the data breach that targeted the City of Helsinki and the deviation management procedures. The Ministry of Education and Culture finds that the report also contains valuable lessons for organisations concerning cyber security development, risk management and management of deviations. Its contents also contribute to supporting the Ministry of Education and Culture in planning potential further measures in its administrative branch.

The Ministry of Education and Culture notes that considering the ministry's substance area, the draft investigation report does not contain explicit information that would jeopardise the realisation of security arrangements or otherwise be unsuitable for a public document. However, the Ministry of Education and Culture points out that the report contains very detailed descriptions that may result in further and even significant reputational damage for the City of Helsinki as well as influence the targeting or selection of the City as a victim of various cyber attacks in the future. In the Ministry of Education and Culture's view, the public version of the document could contain a more general and briefer description or summary of the course of events and factors that led to a successful data breach.

Regarding section 5.1 of the recommendations, the Ministry of Education and Culture notes that in addition to those discussed, problems in practical application may come up in situations where personal data are processed between different administrative branches. An example of this are student welfare services, in which special categories of personal data are processed to perform the statutory tasks of both the wellbeing services counties and education services. The Act amending the Student Welfare Act (377/2022) has resulted in variable interpretation and implementation practices while also adding to the complexity of the information security and information management environment in education services.

Regarding section 5.3 of the recommendations, the Ministry of Education and Culture welcomes the proposal concerning more extensive cooperation, especially with the Ministry of Education and Culture and the Cyber Security Centre. Similar cooperation is also possible on measures aiming to prevent data breaches or to promote preparedness for them. Clear responsibilities as well as communication and reporting practices are an essential part of forming effective cross-administrative situational awareness and deviation management.

The **Finnish Transport and Communications Agency Traficom** has structured its statement around four points: the statutory tasks of Traficom's Cyber Security Centre, the Cyber Security Centre's actions in the case, the Cyber Security Centre's cyber services, and comments on the conclusions and safety recommendations.

Traficom points out that its statutory tasks relating to cyber security are only partly described in the investigation report and elucidates in its statement these tasks, cooperation between Traficom and other authorities, as well as collaboration in different cyber incidents. Traficom additionally brings up the fact that cooperation between the authorities investigating data breaches is effective and routine but should be further developed and practised.

Traficom stresses in its statement that the investigation report should include not only the Cyber Security's Centre's operative cyber security tasks but also its oversight duties related to cyber security laid down in section 303, subsection 1 of the Act on Electronic Communications Services (917/2014). Traficom additionally points out that under section 26, subsection 1, paragraph 1 of the Act on Cyber Security, which is based on the NIS 2 Cyber Security Directive, and section 18h of the Information Management Act, it is the oversight authority in several sectors.

Traficom also notes that the investigation report gives a misleading idea of certain cyber security services offered by the Cyber Security Centre to the public sector and adds detail to this topic in its statement.

In the context of the report's conclusions, Traficom points out that both proactive guidance measures and retroactive control are stressed in the oversight authority's tasks. Proactive guidance is better placed to reach the supervised organisations within the limits of the oversight authority's resources. In Traficom's view, proactive guidance is an effective oversight measure in the field of cyber security. The oversight authority's guidance measures do not, however, preclude the use of other tools of control. Traficom notes that if the oversight authorities had many times larger resources compared to their current ones, fundamental changes to retroactive control could also be considered in different sectors, including inspections of supervised organisations. The resources allocated to different authorities for cyber security control and guidance tasks are, as a rule, very meagre in Finland.

Traficom agrees in its statement with the view that the public sector's cyber security and capabilities for responding to the threats of different cyber offences should also be developed in the years to come. Traficom finds that the preconditions for this would include, in particular, allocation of resources to actions and personnel for improving cyber security, training as well as deployment of the necessary technical methods. Traficom finds that significant investments should be made in the public sector's ability to respond to serious national threats but also threats from cyber criminals. According to Traficom, this could include particular investments in methods for observing and responding to attacks and vulnerabilities, such as the Cyber Security Centre's HAVARO and Hyöky services.

Traficom notes that also in the public sector, the organisation carries the ultimate responsibility for maintaining and developing its information and cyber security. Traficom stresses that the cyber security processes and methods used in the public sector should also be reviewed in the light of the new Act on Cyber Security and amendments to the Information Management Act.

Traficom points out that the Act on Cyber Security, which has recently entered into force, and amendments to the Information Management Act also impose new obligations on public sector actors.

Traficom supports the proposed safety recommendation (recommendation 5.2) as, from the viewpoint of improving Finland's national cyber security, developing the ability to detect information security shortcomings in the public administration can be deemed a key measure for a more cyber secure Finland.

The **Finnish National Agency for Education** provides further information on the guides and instructions published by it in its statement. The Agency stresses that it is not competent to issue orders on the interpretation of the data protection legislation, which is why the scope of its guides and support materials depends on the available case-law and the oversight authority's decisions. The Agency proposes that its role be worded in the recommendation in a way that corresponds to its mission, for example stating that the Finnish National Agency for Education supports education, training and instruction providers in developing clear and accessible instructions on communication about data breaches.

The **Digital and Population Data Services Agency** notes in its statement that the current statutes are sufficient for maintaining information security and that the basic legislation on this matter is adequate. According to the Agency, the challenges lie in awareness of the stat-

utes and resources needed for full compliance with the requirements. The Digital and Population Data Services Agency finds that, rather than increasing supervision, it would be more important to support and guide actors in fulfilling the statutory requirements.

The **Data Protection Ombudsman** draws attention to the use of certain concepts and judicial details in its statement and requests that they be used more accurately. The Ombudsman notes in the statement that the report does not contain all measures the Office of the Data Protection Ombudsman took in relation to the case. The Office of the Data Protection Ombudsman also draws attention to the fact that, while the Data Protection Ombudsman does have regular supervisory activities, the Office would need better resources to place more emphasis on them.

The **Ombudsman for Children** notes in their statement that the investigation report is clear and detailed and provides an excellent understanding of the data breach, its investigation, communication as well as the conclusions and recommendations. According to the Ombudsman for Children, the investigation report has succeeded well in identifying the need to address age-appropriate communication at children and young people concerning the data breach and protecting yourself from its consequences as well as keeping your personal data safe. The Ombudsman for Children points out that under section 5 of the Finnish Data Protection Act (1050/2018), the age limit applied to offering information society services to a child is at least 13 years.

The **City of Helsinki** finds in its statement that the account of the data breach events and the conclusions drawn on it are useful, as this information can in the future be used to support the development of information security, information management and data protection. The City of Helsinki considers that the investigation report is a well executed and comprehensive account of the events.

In the City's view, the data breach was professional, well planned and effectively carried out. The City of Helsinki estimates that the victims numbered approx. 150,000 learners and their guardians as well as all 38,000 employees of the city.

The City of Helsinki justifies the selected communication policy in its statement. In the initial phase, informing all data subject personally was deemed impossible, which is why the City resorted to a public communication allowed under the General Data Protection Regulation. The City of Helsinki notified its decision and information actions taken to the Data Protection Ombudsman. The City of Helsinki stresses that it regularly assessed the possibilities of informing data subjects personally during the data breach and its investigation, but as identifying the leaked data with sufficient accuracy was not possible, it was deemed that adequate preconditions for personal information provision did not exist. Neither did the Data Protection Ombudsman direct the City to do otherwise.

The City of Helsinki notes that, considering that the investigation remained incomplete, external communication on a tighter schedule would not have been possible. The City brings up in its statement the view that, while instructions had in practice been issued for deleting outdated files on the network drive, compliance with the instruction was not controlled.

According to the City of Helsinki, not only statutes that focus on a narrow area but also authority divided between competent office holders in the municipality fragment the procurement and development of information systems needed to provide services. A precondition for managing a modern and secure ICT architecture is centralising decision-making relating to technologies and core information systems. This is another factor that makes it difficult for

those responsible for information management to understand the requirements as a whole and leads to their inconsistent application.

The City of Helsinki considers the issued recommendations necessary, however rather sweeping, which may make implementing and controlling them challenging. The City finds justified the aim of developing the proactive detection and rectification of shortcomings in information security.

The City regards the section on developing instructions for communication as problematic because under section 121 of the Constitution, responsibility for developing a municipality's communication rests with the municipalities themselves. The authorities can support the municipality in this task but not take it over. The City finds support provided by the Association of Finnish Local and Regional Authorities in identifying and rectifying information security gaps and developing information security a very good idea.

In the context of schools' information security, the City of Helsinki points out that the high number of learners who are still minors when attending basic education creates a significant challenge to information security in school environments, especially in larger municipalities. In the City's view, the investigation report has not paid sufficient attention to the perspective that the development of pupils' and students' information security skills comprises not only attaining the objectives of the curriculum but also maintaining the information security of the organisation's systems. The City of Helsinki notes that the Finnish National Agency for Education should include developing children's digital skills in the curriculum and draw up instructions for addressing information security in situations where the pupils' poor digital skills create a risk for their environment.

The City of Helsinki finds the questions of damages associated with a large data breach significant as, in addition to direct damage, justified fears of potential leaks of personal data or their future misuse may entitle a person to compensation. Paying compensation for non-material damage may turn out to be as costly as that for material damage. Consequently, even a minor shortcoming in information security or negligence may result in far-reaching and expensive damage. It is important that compensation for damage is paid pursuant to legislation and based on a causal relationship and proven damages, ensuring that regulation or compensation practices do not become overwhelming.

The City of Helsinki also adds minor details to the course of the events.

DigiHelsinki Ltd notes in its statement that it has provided firewall services in accordance with the service description of the framework contract and that the service did not include monitoring of security alerts. According to the statement, the ASA 5515 used in the data breach was at no time under DigiHelsinki's control and the company had no visibility over the device or KASKO's internal network. DigiHelsinki had made a tender for the installation service of the telecommunications equipment and accordingly contracted Dustin Ltd to upgrade the certificate ordered by KASKO. In DigiHelsinki's view, the ownership and maintenance of ASA 5515 belonged to KASKO. In addition, DigiHelsinki's statement provides clarifications regarding the handling of anti-malware alerts and tickets.

According to its statement, the **Association of Finnish Local and Regional Authorities** finds it useful that the course of events in the data breach targeting the City of Helsinki has been investigated and that safety recommendations to prevent the recurrence of similar events have been identified in this context. What the Association deems particularly laudable is the detailed description in the report of how the data breach progressed and what the reasons behind its success were. According to the Association of Finnish Local and Regional Authorities,

this description can be used to support the development of information security and data protection in municipalities. The Association proposes that, based on this description, a detailed list of development areas be directly drawn up for each organisation.

The Association finds the recommendations included in the report important. However, they are considered sweeping and general in many respects, and their practicability is consequently questioned. The Association of Finnish Local and Regional Authorities stresses in its statement the importance of good information management for effective and correctly targeted information security and data protection measures. It notes that while the volume of legislation and different guidelines is large, they are scattered and the municipalities receive little or no support in their application directly from the authorities.

In the Association's view, the degree to which the recently increased understanding of the municipalities' role in national preparedness and the critical nature of municipalities' personal data pools should be visible in national cyber security strategies, action plans and funding decisions needs to be considered. The Association believes that the current state of information management is not necessarily as problematic as the report indicates.

The Association points out that realisation of chapter 4 of the Information Management Act containing information security requirements is not evaluated by anyone. The Association of Finnish Local and Regional Authorities finds it important to solve this problem of legislation and its enforcement in order to make it possible to initiate and conduct over the long term evaluations of whether or not chapter 4 of the Information Management Act is realised.

The **National Bureau of Investigation** puts forward a technical correction to the investigation report concerning its organisation. Otherwise it had no comments to make.

The **Ministry of Justice** had no comments on the investigation report.