GDPR compliance for a small company

Sonja Korhonen

2025 Laurea

Laurea University of Applied Sciences

GDPR compliance for a small company

Sonja Korhonen
BIT Cybersecurity
Thesis
May, 2025

Laurea University of Applied Sciences

BIT Cybersecurity

Bachelor of Business Administration

Sonja Korhonen

GDPR compliance for a small company

Year 2025 Number of pages 23

Abstract

The objective of this thesis was to analyse the privacy compliance practices of a small company. The company requested a privacy audit and notice. Adhering to GDPR regulations is a requirement for all-EU based companies. This project aimed to provide recommendations for the company to help them to be more compliant.

The theoretical framework used was the General Data Protection Regulation (GDPR), as the company is based in two EU member countries. The research methods included the collection of primary data, observation of the current workflows and practices, review of existing documentation and the analysis and development of best practices accordingly.

The key findings were the lack of documentation, and how the company website omitted to collect consenting information. The defects were rectified as a result of this project, and the privacy notice was placed on the company website. The recommendation was to create clear written instructions for the employees for correct data handling and retention practices, a record of processing activities, data breach situations and a listing of third-party processors.

Keywords: GDPR, GDPR compliance, data privacy, small business compliance

Contents

1 Introduction

The importance of data protection has increased as businesses are more and more data driven. The General Data Protection Regulation (GDPR) has been developed for the companies operating in the EU area to adhere to privacy laws, and to ensure that the private data is handled correctly. This thesis focuses on analysing GDPR compliance practices of a small company. To analyse if the data handling processes are compliant, an internal audit was performed. The audit found some items that needed to be rectified for the company to be fully compliant. The second objective of this project was drafting a privacy statement to be used on the company website. Compliance is an important part of the company structure, and needs to be ensured, even if (or especially) when the company is small. Small companies don't usually have the resources to have legal employees or departments, so employee awareness becomes the most important part of the compliance process. This thesis will explain the background of the company, the objectives, theoretical framework, key concepts and then go into the internal auditing process. The auditing process included explaining the risks and restrictions of the company, but also the results and outcomes relating to the objectives. The privacy notice was drafted in English for the company's use. Small companies have the same responsibilities but not the same resources to adhere to GDPR. Therefore, it's important to ensure an easy and ongoing practice to help the small company to stay compliant with privacy laws.

2 Background

The client company specialises in certification test center operations and other relevant certification processes in Finland and Sweden. The company also offers consulting for processes regarding testing environments, security and test proctoring. The company is privately owned and employs four people (in January 2025). The company was separated from its parent company in 2020 as its own business. Its yearly revenue is around 200 000€ (Kauppalehti, 2025). GDPR.eu (2019) states that around half of small businesses fail in being GDPR compliant, especially in data processing activities and their documentation, and in offering a clear lawful basis for data processing. This statistic is understandable as small companies might not have the means to hire legal departments. Most small companies stated fines being the main reason for GDPR compliance (GDPR.eu, 2019), but it's also an ethical question. Handling customers' private data correctly and ethically is also a question of value. The company name is not published in the final draft of the thesis according to the client company wishes. The challenge of the client company is that the employees handle personal data daily but lacks instructions on how to do it correctly. As the client company has only four

employees in total, the more classic hierarchical way of dividing the employees is not realistic. The division helps bigger companies to restrict access to personal data handling.

3 Objectives

The project was started by coming up with two main objectives for the client company. The client wished for a privacy audit, and a privacy notice. The need for privacy audit was to analyse if the company is compliant with privacy laws, and to find gaps in the knowledge and processes. Privacy notice is something that the client company knew they didn't have and is required by the regulations. This was to be published on the company website, and to notify the relevant stakeholders of the privacy practices of the client company.

3.1 GDPR Compliance Audit

The objective of this project is to perform a GDPR audit for the company, and to analyse if the relevant privacy laws are adhered to. To start the audit, the relevant GDPR Articles need to be recognised. The current data handling methods need to be analysed, and the best practices to correct methods of handling private data moving forward need to be found. The auditing is needed to determine which parts of the company's private data handling need to be evaluated and possibly corrected. The company handles private data of customers daily, but there's no clear communication on how it should be done correctly. Based on the observation and analysis of current practices, the audit checklists are determined, and the audit is performed. This also includes analysing the risks associated with current practices. According to Information Commissioner's Office (2024a) all companies are accountable for handling their customer (and employee) data in a lawful manner.

3.2 Privacy Notice

The second objective of this project is to draft a privacy notice for the company's use. Privacy notice is important because it informs the user (customer) their rights, how their data is being processed and how to control or use those rights. According to Articles 5 and 6, all companies must provide a lawful basis to collect and handle personal data. And since this is the main issue in small companies (GDPR.eu, 2019), this was an important objective for this project.

4 Research and development methods

To determine how to approach the objectives, the research methods were determined. As the company is small, it's relatively easy to observe all the employees in the operation. These observation instances also included a conversation of the workflow practices. The main theoretical framework is General Data Protection Regulation (GDPR) as it's the main privacy regulation within the countries that the client company is operating. With GPDR it's also important to take the country-specific laws into consideration. In this case, the client company operates in two EU member countries, Finland and Sweden.

4.1 Theoretical framework

For this project, the framework used is General Data Protection Regulation (GDPR). The GDPR is a holistic framework to ensure that businesses have the responsibility to carefully process and store personal data. It also covers the rights that the data subjects (users) have for their personal data.

4.1.1 General Data Protection Regulation (GDPR)

According to the European Union (2016), The General Data Protection Regulation (GDPR) is a regulation based in the EU that protects individuals' rights in their own private data. Rights to one's personal data is considered a fundamental right within the EU. However, the right to protection is related to the data's relation to its function in society. This means that there might be instances where a person's right to privacy is weighed against public interest. In general, GDPR makes sure that an individual has rights against companies when it comes to handling and storing their personal data. For this project, the more relevant Articles are relating to companies' accountability and responsibility when it comes to storing and handling customer data.

Relevant GDPR Articles:

Article 5: Principles related to processing of personal data (lawfulness, fairness, transparency, etc.). For small businesses it means that all the data collected needs to be done responsibly, the businesses only collect necessary data and limit the storage and keep the data secure. The company is also accountable for the processing of the data and of the consequences (European Union, 2016).

Article 6: Lawful bases for data processing. For small businesses it means that they need to choose and document any valid reasoning behind collecting personal data (European Union, 2016). For small businesses this could mean restricting the data that is being collected. The customers might voluntarily provide a lot of data to help the business provide the service. It's important to remember not to store this additional data "just in case", as there is no lawful basis to store it.

Article 12, 13 and 14: Privacy notice (transparency, communication, rights management etc.). These articles relate to the businesses' responsibility to communicate what data is being collected, why and where. The users must be explained their rights in simple terms (European Union, 2016). These articles are important especially for the drafting of the privacy notice.

Article 30: Record-keeping of processing activities. This article relates to small businesses' responsibility to keeping internal records of the data processing activities, for example what data is being collected, why and who has access to it (European Union, 2016). This could include a data access matrix, data retention plan, offboarding practices etc.

Article 32: Security of processing. The data that the company collects needs to take measures to ensure that the data is kept securely. This can include tools like passwords, rights management, firewalls or software (European Union, 2016). For small businesses this is a more straightforward way to ensure that the data is safe, without needing to have a legal team.

Article 33 and 34: Data breach notification procedures. These articles relate to what is done in case of data breach, and how the data subject (user) is notified (European Union, 2016). The local data protection authorities in Finland and Sweden consider these articles very important.

4.1.2 Key concepts

Key concepts are explained to help understand the project in a more generic sense, but also regarding this project.

Accountability

Accountability refers to the responsibility that (for example) companies have in reference to handling personal data (Information Commissioner's Office, 2024a). For this project, accountability means that the client company is accountable for handling users' personal data with integrity and communicating that with the users in a clear way. This is stated especially in Article 5 and is relevant to the privacy notice.

Correct data handling

Correct data handling refers to ways to make sure that the data gathered and processed is used in a correct way, and kept safe (Cyrino, 2024). For this project correct data handling takes safety and best practices into consideration and observes the current workflow to determine if something needs to be changed. Correct data handling also includes checking that no unnecessary data is being stored or processed without a lawful basis.

Data processing

Data processing refers to operations in which personal data is processed. Examples of data processing include payroll administration, companies collecting customers phone numbers, posting a photo of a person (in which they can be identified in) online (European Commission, 2023a). For the purpose of this project, all the operations where data is being processed need to be named and determined in a clear way.

Data retention

Data retention refers to the practices in when to keep or delete personal data in the company's systems. Irrelevant or outdated data needs to be deleted in a timely manner (Information Commissioner's Office, 2024b). Especially data retention needs to be considered for this project, as the client company has no clear instructions on how to delete irrelevant or outdated data. This also includes making sure all the client information is up to date and checked regularly. If systems create automated backups, data retention needs to be considered, as some outdated data might end up in the backup versions of datasets.

Personal data

Personal data is any information which relates to an individual and with which said individual can be identified. Examples include the individual's name, phone number, address, IP address etc. If the data is encrypted or anonymised, it's not considered to be personal data. Also, data relating to companies or corporate entities is not considered personal data (European Commission, 2023b). This project might use the terms private data and personal data interchangeably.

Privacy notice

According to the Information Commissioner's Office (2024c), privacy notice is needed if a company holds or handles personal data. Privacy notice is drafted to inform all stakeholders in which way personal data is handled and processed. It is also important to include the data retention time, and who has access to it.

Test provider

Refers to the global companies that provide tests for the individuals taking the exams in the test center. This term is added to the key concepts to explain the client company operations.

4.2 Data analysis methods

For analysing and developing the project, the data management plan was drafted. For this project, it was important to also decide how the client company data was used. The client company wished to keep as much of the project material only available on the company systems as possible. To ensure this, no auditing or interview notes were handled outside the client company systems.

4.2.1 Data management plan

For the purpose of this project, personal data is not being collected or processed outside of the company's own systems. This means that no sensitive data is part of the thesis project. All investigations and observations were conducted internally and are left out of the process documentation. Three employees were interviewed, and the workflow was observed on three different days. The three days were chosen based on the test provider systems the employees were using to get a wholistic view of the data processing practices. The interview was not structured, but more based on observations on the dates. The interview/audit notes outside of the checklists were handled in the company's own systems for security purposes and will be left unpublished for this thesis. The interviews and observation dates were not structured as the company only employs three people, excluding the CEO. The observations were thought to have more insight in a conversational way than in a structured way, due to the small sample size. The restriction of the audit and interview notes is also to ensure that no sensitive information or personal data is being handled outside the company systems. This relates back to Article 5 and 6, as the company is accountable for the correct data handling.

4.2.2 Collection of primary data

To understand how private data is currently being handled in the company and what needs to be improved for compliance, primary data needs to be collected. The current documentation is reviewed, and the systems in which data is handled need to be mapped. The current workflow is to be observed and analysed. All employees (excluding the CEO) were interviewed regarding the daily tasks along the observation process. As mentioned in chapter 4.2.1, the

observation and interviewing situations were not structured due to the small sample size of employees that the company has.

4.2.3 Analysing and developing

After primary data had been collected, the data was analysed according to the articles mentioned in chapter 4.1.1. After the analysis, the recommendations for required documentation were listed. The recommended documentation is under chapter 5.3.3. The recommended documentation could be collected into a privacy handbook that would be easier to use and would become familiar to the employees.

4.3 Internal auditing

Based on the collected primary data, the following objects are selected for the internal audit: IT systems, data retention, third-party processors (cloud storage), data access and employee awareness. These objects were selected with the help of the client company employee team.

4.3.1 Checklists for auditing

IT systems

- Are strong password rules and two-factor authentication in place where possible?
- Are there regular backups?
- Are firewalls, software updates and antivirus software up to date?

Data retention

- Are the retention policies documented?
- Is there a clear retention schedule for old data?
- Are employees aware of how and when to delete old data?
- Is there a retention schedule for old backup data?

Third-party processors (cloud storage)

- Are Data Processing Agreements (DPAs) in place for third parties?
- Are all third-party processors GDPR-compliant?

- Is there a list of external data processors?
- Is any personal data transferred outside the EU/EEA and is proper safeguards in place?

Data access

- Do access rights adhere to least privilege principle?
- Is there a clear offboarding process for previous employees?
- Are system audit logs kept and reviewed to detect any possible unauthorised access?

Employee awareness

- Have employees received GDPR training?
- Do employees know what a data breach is and what to do if it happens?
- Do employees know how and where to handle data correctly and when it should be deleted?
- Is there internal documentation on GDPR best practices?

Objects for audit	Criteria	Data collection method	Findings	Recommendations and notes
IT systems	Backup processes, encryption, security (Article 32)	Interviews, documentation review, workflow observation, notes	Most local data is handled within the company Microsoft cloud/products. Company uses 2-factor identification, passwords and firewalls to ensure security. Backup processes are automated.	Documentation on data retention best practices. Audit checklist: ok.
Data retention	Schedules for retention, data deletion processes	Documentation review, interviews	There's no up-to-date data retention documentation, no clear schedule, no backup retention schedule (unless automatic)	Documentation on data retention best practices. Audit checklist: needs review.

Objects for audit	Criteria	Data collection method	Findings	Recommendations and notes
Third-party processors (cloud)	Vendor GDPR compliance	Contract review, vendor assessment	No list of third-party processors was found. In most situations, the third-party processors were the test provider companies (data controllers). No DPA listings.	Ensure using the cloud for all work-related documentation. List of systems where data is being processed. Audit checklist: needs review
Data access	Access rights management, audit logs, least privilege	Audit reports, access list review	The data access management is up to date. Offboarding practices are up to date. System audit logs are not reviewed regularly. No change of personnel recently.	No improvement recommendations on data access (See restrictions 4.5). Audit checklist: ok
Employee awareness	GDPR knowledge, breach response awareness, data handling practices	Interviews, workflow observation	The employees have a high understanding of privacy laws. No high-risk issues were found due to employee activeness. There is no internal documentation on GDPR best practices. A daily GDPR compliance checklist could be a useful tool to add.	Documentation on privacy related best practices. Audit checklist: needs review.

Table 1: Auditing table

4.4 Audit risk assessment

IT systems

The IT systems were up to date when it came to security. If any personal data is downloaded locally to the computers, the deleting needs to be ensured. This includes emptying the recycling bin, regular checkups on “Downloads”-folder etc. Especially these kinds of things should be added to a daily compliance checklist as they are easy to forget.

Data retention

As there was no documentation on data retention practices, the data might be stored for too long locally. The data that is being handled outside the test provider systems is more likely to be forgotten for the data retention cycle. Outdated data could be forgotten locally and therefore is more subject to data breaches. The risk of retaining data for too long is higher if there’s no relevant documentation on data retention practices. Especially Finnish and Swedish data protection authorities are interested in Records of Processing Activities (ROPAs).

Third-party processors (cloud storage)

There wasn’t a comprehensive list of third-party data processors. The risk is that not all vendor contracts would be vetted periodically. Some vendors can update their terms of service, and some data could be leaked or be transferred in a way that doesn’t adhere to privacy laws (like anonymization of data).

Data access

System audit logs should be reviewed for unauthorised access purposes regularly. The offboarding practices were up to date, as there hadn’t been any changes in personnel in a few years. As there isn’t a huge turnover of employees in the company, it’s important to have process documentation on what should be done if an employee leaves.

Employee awareness

There are no official instructions for the employees on how to handle private data correctly. This is a risk, as there might be errors in how to handle certain documentation with personal data. Also, the lack of documentation is noticeable when it comes to practices on possible data breach situations. This could lead to severe consequences for both the client company and the user whose data is being processed. The lack of documentation could also lead to mistakes on the employees’ part, especially on data retention and deletion of documents locally.

4.5 Restrictions

When personal data is being handled in a small company that employs a very small number of people, in this case four, it's hard to restrict which data should be handled by which employees. If an employee is out of the office for a vacation or due sickness, it's important to ensure business continuity. Therefore, it's not realistic to divide the employees in a clear hierarchical way, like in bigger businesses.

Due to the size of the company, there are also no employees specifically appointed to ensure compliance. However, this does not exempt the company from being compliant with the GDPR regulations and requirements.

In general, due to the small size of the company it might be difficult to ensure complete reliability of results and ethics. If the number of employees was bigger, it might be easier to have a more reliable reflection on the results of this project. For this specific project, the interest was to make data privacy and GDPR work for this company, so the results of the audit and analysis might not be scalable and adaptable for other companies.

5 Results and outcomes

The results of the auditing process revealed some needed improvements in certain areas. These results are included in the next chapter. The next chapter also includes some insights into the auditing notes that were collected during the observation process.

5.1 GDPR Compliance

The auditing process included listing all the possible ways that the company employees would handle private data outside of the test provider systems. Some personal data is being processed in different and separate systems. The company runs exams for six different global test providers. Each of them has their own system, in which the data is handled. In these cases, the client company is only a data processor, and the client company is adhering to the rules that the test provider companies have set up. The data controller in these situations is the test provider company. The client company has no reasonable doubt to think that the test taker companies are not adhering to the European Data Protection laws. In these cases, the client company might collect the test taker's signature, palm vein scan and picture, but it does not save the information on the client company's own computers. This can also mean

having log sheets that need to be destroyed in a certain number of days. These practices seemed to be adhered to daily when the audit was conducted. The employees found the paper-based log sheets an outdated practice that the test provider company was still relying on. The employees were taking good care of the retention of the paper trail. (Audit notes, 2025). This part of the observation process added to the need to have a comprehensive list of all vendors and systems that the employees use. When it comes to the test provider companies, if any issues with data privacy laws were found, the entity responsible would be the test provider.

In some cases, the client company employees make reservations for the test takers and contact the client company to book the appointment, which is then invoiced to their employer company. The data is voluntarily sent by the user and is only used to provide the service. According to the Information Commissioner's Office (2023) the auditing should start by listing which information is needed and what for. The client company collects the following information from the test takers: Name, phone number, test name, test taker ID (if available) and invoicing details. There's a lawful basis to collect this information: name, test name, test taker ID is needed to book the exam, phone number in case there's a problem with the booking, and invoicing details to invoice the service. The information is recorded in Outlook (email and calendar). Email because there needs to be written confirmation for the service and its price, calendar, so that the employees know when to book the exam. The information is then transferred to a sales program called Pipedrive and invoiced through Fennoa. The old calendar notes should then be deleted after the invoice has been paid. In the audit, the old calendar notes had been removed from 2023. This is due to the diligence of the employees. There weren't any official instructions to ensure that the outdated information should be deleted after a certain amount of time. Old emails were not being deleted in a timely manner. There is no lawful basis for keeping old emails, as all the important information relating to the reservations is recorded in the invoicing system. The old emails should be deleted. It might be reasonable for the client company to place an automatic deletion rule for the email inboxes. If the data was not handled in the test provider systems, it was handled in the company's own Microsoft cloud.

The other point that the Information Commissioner's Office (2023) mentions is that security is important, especially if any sensitive information is handled. Since the information is usually linked to people's professional lives, not any sensitive information is gathered. The phone number is the most sensitive piece of information in this case. The phone number is only used in problem situations. The phone numbers are not saved on any of the company phones.

The test center also has CCTV on premises to secure the test environment. There are two separate CCTV systems, one controlled by a test provider company, and one controlled by the client company. Altogether, the test center in Espoo has 15 cameras. Two of those cameras

are controlled by the client company. Both camera systems automatically delete the surveillance data after 30 days. The data retentions practices are in place for the CCTV practices. All customers taking an exam are made aware of the CCTV recording, and it's a part of the agreement that each of them must agree to take the exam. This information is also sent to the customers before the exam date.

The internal audit revealed that three out of the five selected objects for auditing needed review. As stated in chapter 4.3, the following five objects were selected for the internal audit: IT systems, data retention, third-party processors (cloud storage, data access and employee awareness. IT systems and data access passed the audit checks, but more detailed documentation on the systems and processes needs to be developed. For data retention practices, documentation on data processing activities and deletion needs to be added. For third-party processors, including cloud storage, the contracts need to be reviewed. Also, a list of all the systems where employees might be processing personal data needs to be added to the documentation. For employee awareness the main issue was a lack of documentation on best practices. Even though the employees were in general very knowledgeable of GDPR practices, instructions would help to ensure day-to-day compliance. The recommendations for added documents are under chapter 5.3.3.

5.2 Privacy Notice

Privacy notice needs to be available for all relevant stakeholders for companies that handle private data. The privacy notice needs to include:

1. What personal data is collected
2. The purpose of processing
3. The legal basis for processing
4. Data retention periods
5. Data subject rights

Articles 12, 13 and 14 of GDPR explain how to draft a privacy notice for the company. The template provided on the GDPR.eu website was used to write the privacy notice for the client company (GDPR.eu, 2020). The privacy notice also uses articles 5 and 6.

According to the Information Commissioner's Office (2025), we can get guidance on how to draft the privacy notice for the company. One of the key issues for the client company was that it is based in two countries, Finland and Sweden. Both countries adhere to the same regulations as they are both EU members. Finland and Sweden have some differentiating privacy related laws, but the laws relating to companies are similar. The main point regarding

local laws is that the privacy notice should be available in local languages (Finnish, Swedish) and in English. The regulations and instructions relating data breaches and language used is stricter in Finland than Sweden, so if the Finnish regulations are taken into consideration, the Swedish market is also covered. Both countries expect clear written documentation regarding possible data breaches and the notification process to the data protection authority (DLA Piper, 2024a, 2024b).

The privacy notice was drafted and placed on the company website during this project. As the privacy notice was being written, the company checked which cookies the website was collecting, and it was noticed that the website didn't include popup to consent to the cookies. This was rectified because of this project.

5.3 Recommendations

The recommendations are based on the audit, and the insights on the observation notes. Within the next chapters, all the recommendations for future reference are listed. These recommendations are for the company to become fully compliant with relevant privacy laws and to help the company to maintain everyday compliance easier.

5.3.1 Continuous monitoring and audits

The recommendation based on this project would be to perform an audit on a yearly basis to ensure ongoing compliance. The client company received the auditing checklist for further use. The recommended documentation under chapter 5.3.3 could be gathered as a privacy handbook, so that all the relevant information would be easily accessed and retrieved.

5.3.2 Employee training in compliance and best practices

There should be a clear timeline for data erasure from Outlook and other systems handled by the client company. According to European Union (2016) the client company has a relative right to keep the client data in systems that are not available for the whole staff, for example, the invoicing system.

To ensure the data retention promises, a rule for automatic deletion of emails should be put into place to all the common email inboxes. This is to further automate the compliance

practices. Also, the rules for deleting calendar markings should be written instructions for the employees.

5.3.3 Documentation for the company's use

Privacy compliance best practices

A clear written instructions for everyday privacy compliance checkups, data retention and handling of private data need to be written for the employees' use. This could also include a daily privacy audit checklist.

List of third-party processors

A list of all the systems the company uses needs to be conducted to keep track of where the personal data is being processed and why. This list would help the client company to keep track of the systems where they might be handling personal data, and to review the agreements more frequently.

Data breach practices (Article 33, 34)

Documentation for what to do and who is responsible for notifying the data protection authorities if a data breach has occurred. This is a crucial documentation that especially the Data Protection Authorities in Finland and Sweden are looking for. It's important to make sure that the employees know who to inform if a possible data breach is discovered, as there's timeframes to ensure it legally.

Privacy notice

The privacy notice that was written as a part of this project needs to be translated into both Finnish and Swedish. This is required by the local data protection officials.

Record of Processing Activities (ROPA) (Article 30)

An internal ROPA needs to be put in place where private data handled is recorded systematically. This document is meant for an internal document that helps the organisation to keep track that the personal data handled is done correctly and lawfully. The Finnish Data Protection Authority also provides a template for this. The template was sent to the client company. (Tietosuojavaltuutetun toimisto, 2025).

6 Conclusion

Since the businesses primarily use electronic platforms to handle customer data, it's important for businesses to ensure the correct way to handle private data. The small number of employees is not a reason not to be compliant with privacy laws. The client company found the project to have been fruitful, not just because the compliance was at a good level, but also a few things were found and fixed as a result. The common problem with the compliance process of the client company was the lack of documentation to ensure that the compliance process was in place. However, the employees had a high level of understanding of privacy compliance practices, so no major issues were identified. The project found issues in three of the five categories identified in the audit, and the recommendations for corrective actions were discussed with the client company. The recommendations regarding the documentation that the client company needs could be collected as a privacy handbook for the employees' use. The best practices and instructions on how to handle customers' personal data should be an everyday task.

The client company was overall pleased with the results of the project. Some recommended actions were taken immediately: the privacy notice was published on the company website, popup regarding consenting to cookies was added, the automatic data retention rules were put in place in the common email inboxes. The list of recommended documentation was sent to the employee responsible for the workflow, along with the auditing checklist. The privacy handbook will be conducted as soon as possible. The client company was pleased with the independent delivery of the project and was interested in working with Laurea again in the future.

References

Electronic

Cyrino. 2024. What are the Key Steps in Data Handling? Accessed 13.11.2024. https://www.linkedin.com/pulse/what-key-steps-data-handling-cyrino-qk1bf/

DLA Piper. 2024a. Data protection laws in Finland. Accessed 28.04.2025. https://www.dlapiperdataprotection.com/index.html?t=law&c=FI

DLA Piper. 2024b. Data protection laws in Sweden. Accessed 28.04.2025. https://www.dlapiperdataprotection.com/index.html?t=law&c=SE

European Commission, 2023a. What constitutes data processing? Accessed 21.02.2025. https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en

European Commission. 2023b. What is personal data? Accessed 21.02.2025. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

European Union. 2016. EUR-Lex. Accessed 21.02.2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC#tit_1

GDPR.eu. 2019. Millions of small businesses aren't GDPR compliant, our survey finds. Accessed 29.04.2025. https://gdpr.eu/2019-small-business-survey/

GDPR.eu. 2020. Writing a GDPR-compliant privacy notice (template included). Accessed 19.04.2025. https://gdpr.eu/privacy-notice/

Information Commissioner's Office. 2024a. Accountability principle. Accessed 21.02.2025. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/accountability-principle/

Information Commissioner's Office. 2025. How to write a privacy notice and what goes in it. Accessed 21.02.2025. https://ico.org.uk/for-organisations/advice-for-small-organisations/how-to-write-a-privacy-notice-and-what-goes-in-it/

Information Commissioner's Office. 2024b. Retention and Destruction of Information. Accessed 21.02.2025. https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/retention-and-destruction-of-information/

Information Commissioner's Office. 2024c. Transparency (cookies and privacy notices). Accessed 21.02.2025. https://ico.org.uk/for-organisations/advice-for-small-organisations/frequently-asked-questions/transparency-cookies-and-privacy-notices/#doesmy

Information Commissioner's Office. 2023. Your Beginner's Guide to Data Protection. Accessed 19.03.2025. https://ico.org.uk/for-organisations/advice-for-small-organisations-new-structure-work-not-to-be-put-live/getting-started-with-gdpr/your-beginner-s-guide-to-data-protection/

Tietosuojavaltuutetun toimisto. 2025. Record of processing activities. Accessed 13.05.2025. https://tietosuoja.fi/en/record-of-processing-activities

Unpublished

Audit notes, 2025.

Kauppalehti, 2023. Company details.

Tables