UNDERSTANDING DATA PROTECTION PRACTICES IN THE HEALTH AND SOCIAL CARE SECTOR

A survey on Professionals' Experiences and Training Needs

Tiia Bäcklund

Supervisor:

Carlos Serrão, Associate Professor and Head of Department, School of Applied Digital Technologies (Iscte-Sintra)

Date: February 26th, 2026

Co-funded by the European Union

UNDERSTANDING DATA PROTECTION PRACTICES IN THE HEALTH AND SOCIAL CARE SECTOR

A Survey on Professionals' Experiences and Training Needs

Tiia Bäcklund

Supervisor:

Carlos Serrão, Associate Professor and Head of Department, School of Applied Digital Technologies (Iscte-Sintra)

Date: February 26th, 2026

Co-funded by the European Union

Acknowledgements

I would like to express my sincere gratitude to my supervisor for their guidance, encouragement, and constructive feedback throughout this thesis process. Their expertise and support have been invaluable in helping me refine my work and deepen my understanding of the topic.

I also wish to extend my appreciation to the ManagiDiTH project, whose mission to strengthen digital transformation management in health and social care sector has provided important context and inspiration for this thesis. The project's commitment to advancing digital competence and leadership has significantly contributed to the relevance and direction of my research.

My heartfelt thanks go to all participants who took the time to respond to the survey. Your insights and experiences formed the foundation of this thesis, and your willingness to share them made this research possible.

Finally, I would like to thank the individuals who reviewed and validated the content of the survey. Your careful examination and thoughtful suggestions ensured the clarity, relevance, and quality of the data collection instrument.

Abstract

The digitalisation of health and social care services has increased the need for strong data protection competence among professionals who handle personal information in their daily work. Although legislation such as the GDPR provides a clear regulatory framework, the practical implementation of data protection depends largely on employees' knowledge, judgement, and ability to apply guidelines in real-life situations. This thesis examines health and social care professionals' experiences, perceived competence, and training needs related to data protection, with a particular focus on the effectiveness of current security education, training and awareness (SETA) practices.

The thesis explores how professionals assess their understanding of data protection requirements, how helpful they find existing training tools, and what kinds of challenges they encounter when applying data protection principles in practice. Quantitative results indicate that professionals generally feel confident in their understanding of data protection, although experience appears to strengthen this confidence. Qualitative findings reveal specific areas where competence gaps persist, including the handling of special categories of personal data and the practical challenges of ensuring confidentiality in fast-paced or shared work environments. Participants also expressed a desire for more practical, scenario-based training rather than solely independent reading or self-paced online modules.

The results highlight the importance of aligning organisational training practices with the realities of service user work. By incorporating professionals' perspectives, organisations can develop more effective training strategies, strengthen internal communication, and support a culture in which data protection is actively discussed and integrated into everyday practice.

Keywords: Data protection; Health and social care professionals; Security education, training and awareness (SETA); GDPR compliance

JEL classification: I18; O33

Index

Acknowledgements ii

Abstract iv

Introduction 1

Chapter 1 - Literature review 3

1.1 Foundations of Data Protection Legislation 4

1.1.1. Concepts of Data Protection Under the General Data Protection Regulation 4

1.1.2. Data Protection in Health and Social Care Services 5

1.1.3. Confidentiality, Special Categories of Data and Sector-Specific Legislation 5

1.1.4. Training Needs, Risks and Organisational Obligations 7

1.2. Professional Competence, Education and Digitalisation 8

1.2.1 Continuous Learning and Professional Development 9

1.2.2. Forms of Learning: Formal, Informal and Non-Formal Education 10

1.2.3. Organisational Competence Management and the Role of Leadership 12

1.2.4. Pedagogical Models for Competence Development (Monological, Dialogical, Trialogical) 13

1.2.5. Data Protection Training and Competence Needs in Digitalised Services 14

1.3. Theoretical Framework 16

1.4. Hypothesis 17

Chapter 2 - Methodology 18

2.1. Research Design 18

2.2. Research Approach and Rationale 19

2.3. Data Collection Methods 20

2.4. Participants and Sampling 20

2.5. Practical Implementation 22

2.6. Data Analysis 22
2.7. Reliability, Validity, and Trustworthiness 25
2.7.1 AI Use Disclosure 27
2.8. Justification of Methodological Choices 27
2.9. Alignment with Research Question 28
2.10. Analysis of Open-ended Responses 28
2.10.1. Coding 28
2.10.2. Thematic Analysis 29
2.10.3. Typification 29
2.11. Limitations 29
Chapter 3 - Research Findings 31
3.1. Introduction to the Research Findings 31
3.2. Background Characteristics of Respondents 31
3.2.1. Country of Employment 32
3.2.2. Education and Profession 32
3.2.3. Work Environment / Sector 32
3.2.4. Years of Experience 32
3.2.5. Employment Sector 32
3.2.6. Participation in Employer-Provided Data Protection Training 33
3.2.7. Use of Background Variables in Cross-Tabulations 33
3.3. Understanding of Data Protection Requirements 33
3.3.1. Self-assessed Understanding of Roles and Responsibilities (Q22.1) 34
3.3.2. Understanding of GDPR in Daily Work (Q22.3) 35
3.3.3. Practical Knowledge of Data Protection (Q24.1, Q24.4, Q24.5) 35
3.3.4. Organisational Context: Discussion of Data Protection in the Work Unit (Q26.4) 38
3.3.5. Summary of Findings for Understanding of Data Protection Requirements 38

3.4. Helpfulness of Current Training Tools 39
3.4.1. Perceived Clarity of Training Materials (Q19.3) 39
3.4.2. Perceived Impact of Training on Skills (Q19.2) 41
3.4.3. Importance of Practical Exercises (Q19.6) 41
3.4.4. Experience and Perceived Need for Further Training 42
3.4.5. Summary of Findings for Helpfulness of Current Training Tools 43
3.5. Integration of Quantitative and Qualitative Findings 44
3.6. Overall Summary of Findings 44
Conclusions 46
Answers to the Research Question 46
Practical Implications 47
Strengths and Limitations 48
Recommendations 48
Future Research 49
Bibliographic References and Sources 52
Annexes 55
Annex A Survey Questionnaire on Social and Healthcare Professionals' Experiences and Training Needs 55
Annex B Coding Scheme / Variable List 64
Annex C Qualitative Responses 68
Annex D Thematic Coding of Open-Ended Responses 82

Index of tables and figures

Index of Figures

Figure 3.1 Respondents’ agreement levels on correct processing of personal data, grouped by years of experience. Source: Author's own work 2026. 37
Figure 3.2 Respondents’ agreement levels on whether data protection issues are regularly discussed in their unit, by sector. Source: Author's own work 2026. 38
Figure 3.3 Descriptive statistics for respondents’ ratings of the clarity and ease of understanding of training materials (Q19_3). Source: Author's own work 2026. 40
Figure 3.4 Respondents’ agreement on the need for further data protection training, grouped by years of experience. Source: Author's own work 2026. 42

Index of Tables

Table 3.1 Distribution of responses to Q24.4. Source: Author's own work 2026. 36

Introduction

The increasing digitalisation of health and social care services has intensified the need for robust data protection practices and for professionals who are able to apply these practices reliably in their daily work. As service user information is processed across multiple systems, devices, and organisational interfaces, the competence of employees has become a critical component of lawful and secure data handling. While legislation such as the GDPR establishes clear requirements for the processing of personal and sensitive data, compliance in practice depends heavily on the knowledge, judgement, and everyday actions of the professionals who work closest to service users. For this reason, organisations commonly rely on security education, training, and awareness (SETA) programmes to ensure that both new and experienced employees understand their responsibilities and are equipped to manage data securely.

Despite the availability of training, previous research and practical experience suggest that professionals may still face challenges in applying data protection principles in real work situations. Health and social care environments are fast-paced, unpredictable, and often characterised by competing demands, which can make it difficult to prioritise independent learning or to translate theoretical guidelines into concrete actions. This raises questions about how well current training practices prepare employees to handle personal and sensitive data, how confident professionals feel in their own competence, and what kinds of support they consider meaningful.

This thesis examines these issues by exploring health and social care professionals' experiences, perceptions, and training needs related to data protection. The thesis focuses on how professionals assess their understanding of data protection requirements, how they perceive the clarity and usefulness of the training tools available to them, and what kinds of challenges they encounter when applying data protection guidelines in everyday work.

The research question that this thesis will address is the following:

"How do health and social care professionals understand and apply data protection practices, and what kind of training do they need to strengthen their competence?"

This thesis approaches this question through a mixed-methods survey design that combines quantitative and qualitative elements. The quantitative component provides structured numerical data on professionals' perceptions and practices, while the qualitative open-ended responses offer deeper insights into the reasons behind these patterns. Document analysis, thematic categorisation, and comparison of relevant legislative and organisational sources further support the interpretation of the findings. Together, these methodological choices provide a structured and transparent basis for analysing how the selected materials address the research problem.

Particular attention is given to areas where competence gaps may emerge, such as recognising special categories of personal data or determining when and to whom information may be lawfully disclosed. The thesis also considers the role of organisational culture, including the extent to which data protection is discussed within work units and how opportunities for reflection or shared learning influence professionals' ability to implement guidelines consistently.

By analysing these perspectives, the thesis aims to provide a comprehensive overview of the sufficiency of current training practices and the types of support that professionals find valuable. The findings highlight how employees' confidence in their competence may be shaped not only by formal training but also by experience, workplace communication, and the availability of practical examples or scenario-based exercises. Understanding professionals' own experiences is essential, as training that appears adequate from an organisational standpoint may not fully address the realities of service user work. The results of this thesis can therefore inform the development of more effective training strategies, support organisational decision-making, and contribute to broader discussions on data protection competence within the fields of health and social care and digital transformation.

By focusing on professionals' own experiences, this thesis highlights the practical realities that shape data protection competence in the health and social care sector. Understanding how employees perceive their preparedness, what kinds of challenges they encounter, and which forms of support they find meaningful provides valuable insight into the effectiveness of current training practices. These perspectives also reveal where gaps may exist between formal requirements and practical implementation, particularly in environments where learning is expected to occur independently or under time pressure.

This thesis therefore contributes to a broader discussion on how data protection competence is developed, maintained, and supported within digitally transforming service systems. By examining both the strengths and limitations of existing training approaches, the research offers evidence that can inform organisational strategies, guide the development of more practical and context-sensitive training methods, and support professionals in applying data protection principles with confidence.

The thesis is organised into five chapters. The introduction outlines the background, purpose and scope of the thesis. The first chapter presents the theoretical and legislative framework, including the key concepts and laws relevant to the topic. The second chapter describes the methodology and data collection process in detail. The third chapter contains the analysis and findings, structured according to the themes that emerged from the material. The final chapter discusses the results, evaluates the implications for practice, and provides recommendations for further development.

Chapter 1 - Literature review

This chapter provides the theoretical and conceptual foundation for examining how health and social care professionals understand and apply data protection requirements in their daily work. Because the thesis investigates professionals' self-assessed competence, their experiences with current training practices, and the challenges they encounter in real-life situations, the literature review brings together research on the legal and organisational frameworks that shape data protection, the specific responsibilities associated with handling personal and sensitive data, and the role of training and digital learning in developing professional competence.

These themes are essential for interpreting the research question, which focus on how well professionals feel prepared to meet data protection obligations, how they perceive the clarity and usefulness of existing training tools, and what kinds of gaps or difficulties they experience when implementing guidelines in practice. In addition to legal, professional, and pedagogical perspectives, the chapter also outlines key concepts in quantitative research to support the methodological choices and analytical framework of the thesis. By establishing this multidimensional foundation, the literature review situates the research within the broader context of existing knowledge and provides the necessary background for understanding the findings.

The literature search was conducted using multiple sources to ensure a broad and relevant foundation for the thesis. Searches were performed in Scopus, Google Scholar, Laurea's Finna service, the Vaski library network, and the Finnish Government Publications portal using combinations of keywords such as social and healthcare, social services, healthcare, professionals, GDPR, data protection, competence, competence development, adult learning, lifelong learning, continuous learning, digitalisation, and digital skills. These searches produced a wide range of academic articles, reports, e-books, and physical books.

From Scopus and Google Scholar, a combination of nine articles was initially identified, from which six were included in the final selection. The Finnish Government Publications portal yielded seven publications, of which six were used. Laurea's Finna service provided seven sources, with two selected for the final review. The Vaski library network offered fourteen books, of which eleven were included. In addition, Finlex was used to access five up-to-date Finnish laws relevant to data protection, including the EU General Data Protection Regulation (hereafter GDPR). Three methodological sources were retrieved from the Finnish Social Science Data Archive, and one source was obtained from the Office of the Data Protection Ombudsman.

Although the search process was not designed as a systematic review, the steps taken ensure transparency in how the final sources were selected. The included materials were chosen based on their relevance to the research question, academic quality, and contribution to understanding data protection practices and competence development in the health and social care sector.

1.1. Foundations of Data Protection Legislation

In Finland, the concept of data protection began to emerge during the 1970s, and after considerable debate on the need for general legislation, the first Finnish data protection law, the Personal Data Act (471/1987), came into force in 1988. The EU Data Protection Directive of 1995 laid the groundwork for harmonization across member states. The introduction of the GDPR in 2018 significantly reshaped the legal landscape. The regulation obliges organisations to process personal data only on a lawful basis, for clearly defined purposes, and in line with core principles such as data minimisation, accuracy, and storage limitation (Andreasson et al., 2023; Keller, 2023; Korpisaari et al., 2022).

1.1.1. Concepts of Data Protection Under the General Data Protection Regulation

The concepts *data protection* and *data privacy* are the terms typically used in English when referring to the legal and organisational safeguarding of personal data (Keller, 2023). Andreasson et al. (2023) report that in Finland, *personal data* is legally defined as any information relating to an identified or identifiable natural person. Identification may be direct, such as through a name or personal identity number, or indirect, through the combination of various attributes. The GDPR introduced additional safeguards for the processing of special categories of personal data, which is generally prohibited unless a specific legal exception applies, due to the high risks such processing may pose to fundamental rights and freedoms (Andreasson et al., 2023).

Implemented in 2018, the GDPR represents a shift in the global perspective on data protection. It grants individuals explicit rights over their personal data, including the right to be informed, the right of access, the right to rectification, and the right to erasure. Additionally, it introduces the principles of data protection by design and by default, encouraging organisations to integrate privacy considerations into processes from the outset (Bakare et al., 2024).

In workplaces — especially in health and social care — robust data protection requires not only regulatory adherence but also employee awareness and competence. It is not a task to be “completed” in a single workshop, but an ongoing process tied to evolving technologies and procedures (Keller, 2023; Sorvettula, 2015).

The GDPR establishes strict data protection standards across the European Union, encompassing user consent, data minimisation, and mandatory breach notifications. The GDPR emphasises individuals' rights to privacy, data portability, and the "right to be forgotten," providing a comprehensive set of protections. This can be described as a rights-based approach to data protection (Bakare et al., 2024; Kambala, 2024).

The GDPR is built on seven core principles that guide all processing of personal data. These include lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Together, these principles form the foundation for compliant and responsible data processing across all sectors (European Parliament and Council, 2016).

1.1.2. Data Protection in Health and Social Care Services

When individuals submit private information to governmental bodies through digital services, they have a justified expectation that their data will be handled with confidentiality and care. These expectations are grounded not only in ethical considerations but also in national and international data protection laws that require organisations to maintain the privacy and security of personal information (Chapple, 2024). Andreasson and Ylipartanen (2025) write that embedding the GDPR principles into everyday practices thus enhances both legal compliance and the ethical standards of care. Staff members who are well-informed about these rights and obligations are better equipped to recognise risks, report potential data breaches, and maintain the trust of service users (Andreasson & Ylipartanen, 2025).

1.1.3. Confidentiality, Special Categories of Data and Sector-Specific Legislation

In Finland, service user information is classified as personal data, and its processing is regulated by the GDPR together with several national laws. According to Office of the Data Protection Ombudsman (2026), personal data includes any information relating to an identified or identifiable individual, and all processing activities — such as collecting, storing, using, transferring, or deleting data — must comply with data protection legislation. In health and social care services, the GDPR is supplemented by the *Data Protection Act* (2018), *Act on the Status and Rights of Patients* (1992), *Act on the Status and Rights of Social Welfare Clients* (2000), and *Act on the Electronic Processing of Client Data in Social and Health Care* (2007). These laws establish strict requirements for confidentiality, lawful processing, and secure handling of sensitive information. Office of the Data Protection Ombudsman (2026) emphasises that personal data must always be processed lawfully, transparently, and for a clearly defined purpose, and only the minimum amount of data necessary for that purpose

may be collected. Inaccurate or outdated information must be corrected or removed without delay, and data may be stored only for as long as it is needed to fulfil the intended purpose (Office of the Data Protection Ombudsman, 2026).

Health and social care services represent a particularly high-risk environment for data protection because professionals routinely process large volumes of sensitive personal data, often under time pressure and in rapidly changing situations. The information handled typically includes health data, social welfare records, and other special categories of personal data, the misuse of which may cause significant harm to individuals. Work environments are complex, multidisciplinary, and involve multiple information systems, increasing the likelihood of human error or unauthorised access. These sector-specific characteristics make strong data protection practices, clear organisational procedures, and adequate staff competence essential for ensuring lawful and secure processing (Andreasson et al., 2023; European Parliament and Council, 2016; Korpisaari et al., 2022).

Confidentiality applies to all service user information in health and social care, as even the fact that someone is a service user can reveal sensitive matters. Section 35 of the Finnish Data Protection Act (2018) further establishes a duty of secrecy and a prohibition on the misuse of personal data: anyone handling personal data who learns details about another person's private life, financial situation, or business affairs must not disclose this information unlawfully or exploit it (Voutilainen & Kurvinen, 2024).

The other key professional duties relating to the processing of service user data can be summarised as diligence, the duty of inquiry, accurate documentation, purpose limitation, necessity, and confidentiality. Lawfulness of processing also requires that service users be informed about the processing of their personal data. According to Article 12 of the GDPR, controllers must take appropriate measures to provide the information specified in Articles 13 and 14. This duty of information supports the principle of transparency, ensuring that individuals are aware of the processing of their personal data and their related rights. Controllers are also responsible for monitoring compliance with data protection requirements, for instance through log data (Voutilainen & Kurvinen, 2024).

The Act on Health Care Professionals (1994, Section 17) prohibits professionals from disclosing, without authorisation, any private or family secrets obtained in the course of their duties. This duty of confidentiality continues even after the end of professional practice. The Act on Social Welfare Professionals (2015) does not contain a directly equivalent provision, but under Section 4, social welfare professionals are ethically required to comply with laws governing the rights and status of service users, including the handling of service user data. Thus, service user information in health and social care is classified as special category data under the GDPR, the processing of which is generally prohibited (Lindström et al., 2025).

Ultimately, data protection is more than a legal requirement. It is an essential part of ethical service provision in the health and social care field. By ensuring that staff understand their roles and responsibilities in relation to personal data, organisations not only comply with the GDPR but also reinforce the dignity, privacy, and trust of the individuals they serve. As digitalisation progresses and service ecosystems become more complex, the ability to manage data responsibly will remain a defining factor for both professional competence and organisational credibility (Andreasson & Ylipartanen 2025).

For organisations operating in the health and social care sector, GDPR compliance is particularly critical. In public health and social care, compliance with legislation is particularly important, as the provision of these services constitutes the exercise of public authority under Section 2 of the Finnish Constitution (1999). Ultimately, the controller is responsible for ensuring that processing complies with the law, including the design of information systems and the guidance provided to professionals (Andreasson & Ylipartanen, 2025; Voutilainen & Kurvinen, 2024).

In practice, health and social care professionals must handle service user data with care, as diligence is a cornerstone of lawful processing. In addition, professionals in public service are bound by statutory duties of office, requiring them to carry out their tasks properly and without delay, in accordance with applicable laws, regulations, and instructions (Voutilainen & Kurvinen, 2024).

1.1.4. Training Needs, Risks and Organisational Obligations

GDPR-related training, aimed at reducing the risk of data breaches, represents an adaptation of internal processes to comply with the regulation. Health and social care institutions must implement further adjustments, for example through staff training, to seek a balance between operational efficiency and effective protection of personal health data. Staff training, particularly in data protection, requires updating to align with the new legislation. Internal data protection training for all personnel is crucial, as most data breaches occur internally rather than externally. Insufficient training can lead to internal data breaches, potentially resulting in substantial fines under the GDPR and significant financial losses for healthcare organisations (Addis & Kutar, 2018).

At the practical level, data protection in everyday work means ensuring that personal data of service users, colleagues, and partners is processed securely and only for necessary purposes. Risks may arise from careless conversations in public spaces, improper document handling, or insecure transmission of data. Employers must provide secure systems and tools, while employees are responsible for respecting confidentiality and handling data appropriately. Ultimately, effective data protection is both a legal requirement and an ethical obligation that underpins trust in professional and organisational contexts (Andreasson et al., 2023).

Health and social care services operate in environments where large volumes of sensitive personal data are processed daily, often under time pressure and across multiple information systems. These conditions increase the likelihood of human error, unauthorised access, or accidental disclosure. Because professionals routinely handle health data and other sensitive information, strong data protection practices and adequate staff competence are essential for ensuring lawful processing. The sector's complexity also places significant responsibility on organisations to provide clear guidance, secure systems, and regular training to support employees in managing data responsibly.

1.2. Professional Competence, Education and Digitalisation

Digital competence in the work of service user-facing professionals extends to information management, digital services, information security, the use of artificial intelligence, and online guidance skills. In everyday service user work, these competencies are manifested in handling service user data, using electronic health record systems, and service user communication. In this thesis, digital competence is approached particularly from the perspective of understanding data protection requirements: how employees perceive their readiness to comply with data protection regulations and guidelines in practical service user work. This focus complements the Ministry of Social Affairs and Health's handbook's (2024a) broader observations on digital capability by adding individual experience-based insights into the secure implementation of health and social care services.

The Osaamisella soteen project (Ministry of Social Affairs and Health, 2024b) explored the competencies of health and social care professionals that support the reform of services in both degree programmes and continuing education. In degree programmes, the competencies identified included for instance digitalisation and technology skills. While courses, seminars, and studies are particularly effective for updating knowledge and reinforcing cognitive skills, relying solely on formal training can be limiting. Learners who remain passive or socially disengaged during training may not achieve the full potential of learning or skill development. It is also notable that social interaction during learning is highly significant for some target groups, and not all training should be conducted online. On the other hand, digitalisation increases accessibility, for example, to education in sparsely populated areas (Berisha et al., 2025; Ministry of Education and Culture, 2019, as cited in Ministry of Social Affairs and Health, 2024b; Viitala, 2005, as cited in Helminen, 2021).

As digital systems become increasingly embedded in health and social care work, professionals are expected to navigate complex information environments while maintaining compliance with data protection requirements. Digital competence therefore extends beyond technical skills to include the ability to recognise data protection risks, apply organisational guidelines, and make informed decisions in situations where service user data is handled. Employees' perceptions of their readiness to meet these expectations are central to understanding how well digitalisation supports secure and lawful service delivery. This perspective highlights the importance of continuous learning and practical training that strengthens both technical and regulatory competence in everyday service user work.

1.2.1 Continuous Learning and Professional Development

Short and continuing education courses are particularly suited for developing digital skills. A variety of training formats, including additional, continuing, and specialisation courses, are necessary. Given the rapid evolution of digital tools and services, focusing on teaching specific current systems is not practical. Instead, education should foster students' ability to adopt and utilise diverse service models creatively and provide a framework for integrating technology effectively. This also encompasses knowledge of data protection and relevant legislation (Helminen, 2021; Ministry of Education and Culture, 2019).

For continuing education in the health and social care sector, the need to optimise the use of competencies among professionals from different fields and to expand their application has been identified. Furthermore, it has been emphasised that multidisciplinary and service user-centred practices, along with digitalisation opportunities, should be considered when developing the skills of all professional groups (Ministry of Education and Culture, 2019, as cited in Ministry of Social Affairs and Health, 2024b).

Ministry of Social Affairs and Health (2024b) suggest that the diversity of digitalisation as part of health and social care services is considered throughout the degree programme and strengthened in continuing education. For professionals already in working life, ensuring the identified common competence areas can be best achieved through education where skills are developed through interprofessional collaboration, improving both individual and organisational practices. Competence development in this context includes elements of work supervision; it is process-oriented, interactive, and reflective (Ministry of Social Affairs and Health, 2024b).

Digital skills in health and social care services are considered a generic competence and skill that should be built throughout education. Learning digital skills in health and social care services should start from service user-centredness and multidisciplinary collaboration. Learning environments should

be developed to allow digital skills to be studied in an integrated manner within the content of other course modules (Ministry of Social Affairs and Health, 2024b).

As digitalisation continues to reshape health and social care work, continuous learning becomes essential for maintaining both professional competence and compliance with data protection requirements. New systems, evolving service models, and changing regulatory expectations require employees to update their skills regularly and apply them confidently in service user work. Ongoing professional development therefore supports not only technical proficiency but also the ability to handle personal data responsibly, reinforcing secure and high-quality service delivery in everyday practice.

1.2.2. Forms of Learning: Formal, Informal and Non-Formal Education

According to the Organisation for Economic Co-operation and Development (OECD) (2020, as cited in Helminen, 2021), *continuous learning* refers to work-related learning for individuals engaged in the labour market. This type of learning may include formal education and study aimed at enhancing knowledge and skills for both present and future work. Continuous learning is broader than formal education, which is typically systematic and goal-oriented and usually involves a teacher or instructor together with students. Continuous learning can occur formally (through structured education), informally (through learning at work and in leisure activities), and non-formally (via programmes offered by adult education centres, hobbies, libraries, museums, and similar institutions). Individuals may also acquire knowledge independently, and learning may be either conscious or unconscious (Biesta, 2006, as cited in Helminen, 2021; Ministry of Education and Culture, 2019a, as cited in Helminen, 2021; OECD, 2020, as cited in Helminen, 2021; Ministry of Education and Culture, 2019 as cited in Ministry of Social Affairs and Health, 2024b).

Valleala (2007) and Viitala (2015) (as cited in Helminen, 2021) emphasise that continuous learning is integral to modern working life. Employees must adapt to changing work practices, methods, and service user needs. The selection of training depends on employees' needs, their work roles, and tasks. Short, targeted programmes are suitable for updating and enhancing specific knowledge and skills, while online and web-based learning provide accessible, flexible, and cost-effective options, requiring learner self-direction (Valleala, 2007, as cited in Helminen, 2021; Viitala, 2015, as cited in Helminen, 2021).

Helminen (2021) writes that continuous learning and skill development contribute to workplace well-being. They enhance motivation and increase employees' commitment to their work. Workplaces typically promote continuous learning through organised training sessions. Employers may arrange

short internal training programmes using trainers from within the organisation or hire external trainers or training providers to deliver the programmes (Helminen, 2021).

The Ministry of Education and Culture (2018a, as cited in Helminen, 2021) points out that continuous learning today is understood in a manner similar to *lifelong learning*, encompassing learning that occurs across a person's entire life and in various areas of life. It provides every individual in Finland with the opportunity to enhance their skills and competence throughout their lifetime (Ministry of Education and Culture, 2018a, as cited in Helminen, 2021).

The need for digital skills training in health and social care can be divided into two main areas. First, all current degree-oriented programmes for health and social care professionals should include competence areas related to digitalisation. Second, every working professional should have opportunities to strengthen digital skills in the areas relevant to their daily tasks. This skills development can occur through formal education as well as informal and non-formal workplace-based training and orientation (Ministry of Social Affairs and Health, 2024b).

In a changing and digitalising society, education and lifelong learning are regarded as important success factors. Competence development is necessary to adapt to and promote transitions brought about, for instance, by ongoing digitalisation in working life. Opportunities in workplaces to learn, develop, and apply skills are linked to both well-being at work and productivity. However, the overall share of employer-provided training in competence development has clearly decreased in recent years (Finnish Government, 2020; Lyly-Yrjänäinen, 2025).

Competence reflects the integration of diverse skills, and flexible methods for updating these skills are vital for actors in the private, public, and third sectors. This ensures the conditions for growth both now and in the future. Workplace learning is increasingly characterised by multiple forms of learning. While much of it still takes place informally — through self-study, peer learning, and experiential growth — it also includes short induction or training sessions organised by employers (Finnish Government, 2020).

Competence requirements pertain to the roles, responsibilities, and objectives of both organisations and employees. Organisational competence needs specify the skills necessary for achieving goals and ensuring organisational success. Employees also have competence needs tied to their specific roles and tasks, requiring them to evaluate the skills needed to perform effectively, reach their objectives, and grow professionally. Competence serves as a resource for both individuals and organisations, facilitating successful task completion, goal achievement, problem-solving, work improvement, and overall performance enhancement (Otala, 2008, as cited in Helminen, 2021).

In the context of health and social care work, understanding the different forms of learning is essential for ensuring that professionals can continuously update the digital and data protection competencies required in their roles. Formal, informal, and non-formal learning each provide

complementary pathways for developing the skills needed to navigate evolving technologies, regulatory expectations, and service user-centred practices. By drawing on multiple learning environments, employees are better equipped to maintain their competence, adapt to change, and apply secure and responsible practices in everyday service user work.

1.2.3. Organisational Competence Management and the Role of Leadership

From a collective perspective, competence and its sharing are weak due to both the structure of educational institutions and employment relationships, both of which are variable and fragmented. Developing the digital competence of staff and learners requires systematisation and goal setting, with particular support needed in digital pedagogy. At present, some citizens fall outside society due to insufficient digital skills, making digital exclusion a real phenomenon (Berisha et al., 2025).

Ministry of Education and Culture (2019) state that digitalisation enhances individuals' participation, enables better decision-making, and supports the development of services along with data-driven management. Competencies related to digitalisation are a critical component of both leadership programmes and professional education for health and social care workers. Such training should deepen understanding of how digital solutions can be used to innovate health and social care practices and services for service users, as well as to make informed decisions about personal health and well-being (Ministry of Education and Culture, 2019).

In health and social care work, there is a large group of professionals who completed their degrees at a time when digitalisation was not yet part of curricula. For this reason, continuing education in the workplace is especially important for these professionals. Today, digital skills are part of the work tasks of virtually every Finnish health and social care professional (Ministry of Social Affairs and Health, 2024b).

Effective competence management in health and social care organisations therefore requires leadership that actively supports the development of digital and data protection skills. Leaders play a central role in creating structures, allocating resources, and establishing expectations that enable employees to maintain and update their competence in a rapidly changing digital environment. When organisational practices prioritise continuous learning and provide clear guidance, professionals are better equipped to apply digital tools responsibly and comply with data protection requirements in everyday service user work.

1.2.4. Pedagogical Models for Competence Development (Monological, Dialogical, Trialogical)

To achieve learning objectives, various methods for skills development are necessary. Both degree-oriented programmes and continuous learning initiatives can employ the trialogical learning model, which encompasses monological, dialogical, and trialogical approaches. The monological model centres on individual knowledge acquisition through lectures, videos, and MOOCs, emphasising independent learning (Ministry of Social Affairs and Health, 2024b).

Ministry of Social Affairs and Health (2024b) notes that dialogical learning occurs through participation in collective activities, where cultural practices, communities of practice, and social-material interaction are key. Methods include internships, group work, virtual simulations, and digital Living Labs, with content focused on practical applications, professional development, and context-specific scenarios (Ministry of Social Affairs and Health, 2024b).

In addition, trialogical learning emphasises collaborative knowledge creation among participants, centred on concrete development projects executed collectively using flexible digital tools. The aim is to shift from individual-focused approaches to collaborative practices. These different pedagogical models require tailored methods for skills and competency development (Paavola & Hakkarainen 2025, as cited in Ministry of Social Affairs and Health, 2024b; Paavola, 2012, as cited in Ministry of Social Affairs and Health, 2024b; Ahonen et al. 2020, as cited in Ministry of Social Affairs and Health, 2024b).

The framework of this thesis is built around the digitalisation of health and social care, professionals' data protection competence, and the supporting structures for competence development. As background, the thesis draws on the handbook published by the Ministry of Social Affairs and Health in 2024, which presents up-to-date information on developing digital capability, particularly from a leadership perspective. Chapter 2.4 of the handbook describes a framework in which digital competence is viewed as part of changes in working life, educational structures, digital culture, and societal requirements. The handbook emphasises the role of digital mentors, the importance of networking, and continuous learning. The need for training is illustrated with statistical and qualitative data, highlighting skills gaps, for example, in artificial intelligence and basic digital skills (Ministry of Social Affairs and Health in 2024b).

Together, these pedagogical models offer complementary pathways for developing the digital and data protection competencies required in contemporary health and social care work. By combining individual study, collaborative learning, and shared knowledge creation, organisations and educational institutions can support professionals in applying digital tools responsibly and adapting to evolving regulatory and technological demands. This integrated approach strengthens both individual capability and collective readiness to deliver secure, high-quality services for service users in a digitalised environment.

1.2.5. Data Protection Training and Competence Needs in Digitalised Services

There has been a fundamental shift in the control and ownership of health data, transferring it from physicians, scientists, hospitals, and healthcare institutions to patients. As the nature of health and social care work changes, the required competence has not yet been sufficiently understood, and systematic measures targeting the change are lacking. The 2024 Labor Barometer highlights that, across all sectors, the most significant skills gap in Finland's workforce concerns digital competence.

Digital competence requires continuous updating. The leadership of digital competence, both nationally and regionally, plays the most significant role in increasing competence and managing workforce capability. It is essential to foster a culture of experimentation and actively involve staff (De Hert & Papakonstantinou, 2012, as cited in Yuan & Li, 2019; Haug, 2018, as cited in Yuan & Li, 2019; Ministry of Social Affairs and Health, 2024b; Tene & Polonetsky, 2011, as cited in Yuan & Li, 2019).

Digital services require professionals to acquire new competencies, including learning to use the services, remotely assessing service needs and urgency of care, identifying service users suitable for digital services, ensuring information security and data protection, considering ethical aspects, and maintaining service user safety (Pennanen et al., 2023, as cited in Ministry of Social Affairs and Health, 2024b).

Ministry of Social Affairs and Health (2024b) suggest that it is important to offer staff appropriate learning opportunities and training that meets the digitalisation requirements of their roles. Overall, health and social care staff digital competence and the perceived digital capabilities of work communities are at a good level, but as expected, this varies between individuals and teams. Training needs exist not only in basic skills but also in more advanced areas of digital competence. Professionals have graduated at different times, and not all received digital studies during their formal education. Conversely, recent graduates may have had substantial digital training (Ministry of Social Affairs and Health, 2024b).

Ministry of Social Affairs and Health (2024b) reports that in social services, high-level competence is emphasised in digital services for service users, ethical digital skills, and digital society knowledge.

However, overall use of digital services is lower than in healthcare. In healthcare, data-driven management competence is considered a more important digital skill than in social services. Digital transformation is reshaping, and will continue to reshape, the skill requirements for health and social care professionals. Adopting new service models necessitates that professionals understand their purpose and functionality and actively engage in implementing changes. Additionally, effective change management in health and social care demands the integration of digital skills into professional practice (Ministry of Social Affairs and Health, 2024b).

Work in digital environments requires not only information security and data protection skills, but also strong ethical competence. Furthermore, professionals need critical evaluation skills for digital health and social care services, as well as user-centered development skills, to ensure that the services respond to the diverse needs of service users, and operational environments (Puhakainen & Siponen, 2010; SOTETIE, 2021, as cited in Holvikivi & Lintula, 2022).

In the European DigComp framework, *digital competence* is defined as the capable, critical, and responsible use of digital technology and engagement with it in learning, work, and societal participation. In addition, the definition of digital competence changes continuously with societal development. Also, different stages of life require different skills, so the key is readiness and ability to operate in the digital environment in which the individual currently exists (Berisha et al., 2025). Ministry of Social Affairs and Health (2024b) describe digital competence in health and social care service user work that it involves mastering a diverse and multichannel service environment, including communication via phone, chat, images, and video. Professionals are expected to understand and manage new technologies as part of their daily tasks, which may include guiding service users, conducting remote consultations, providing expert advice, and documenting interactions (Ministry of Social Affairs and Health, 2024b).

Adequate data protection competence among staff can significantly enhance an organisation's productivity, efficiency, and cost-effectiveness. When employees are well-trained and confident in handling personal data, they are more likely to perform their duties effectively, which in turn strengthens both operational and customer processes. Importantly, staff expertise in data protection safeguards service users' trust, as it ensures that personal information is processed appropriately and lawfully throughout its lifecycle. This includes activities such as data collection, storage, use, combination, transfer, disclosure, retention, and deletion (Andreasson & Ylipartanen, 2025).

Furthermore, building a strong data protection culture requires leadership commitment and active communication across all organisational levels. Managers play a pivotal role in modelling compliance and ensuring that staff have sufficient resources to handle data securely. When data protection becomes embedded in everyday practices rather than treated as a separate task, it

enhances organisational resilience and fosters a climate of accountability (Andreasson & Ylipartanen, 2025).

Data protection should therefore not be understood merely as confidentiality or secrecy. Instead, it forms part of a broader strategic framework in which organisations increasingly rely on external service providers and specialised expertise. In this context, well-structured contractual arrangements and clear accountability mechanisms become essential. Data protection is gradually evolving into a core element of strategic management, shaping organisational practices holistically and contributing to innovation, compliance, and sustainable trust-based relationships (Andreasson & Ylipartanen, 2025).

Continuous training and systematic orientation are crucial for ensuring that employees remain competent in data protection issues. Initial induction should introduce new staff to the organisation's policies, technical safeguards, and practical routines, while ongoing education helps to keep their knowledge up to date in light of evolving regulations and technological developments. Training should not only address the legal aspects of GDPR but also provide case-based examples that illustrate the ethical dilemmas and everyday challenges of handling sensitive data (Andreasson & Ylipartanen, 2025).

Taken together, these developments illustrate how digitalisation has transformed the competence requirements of health and social care professionals, ensuring that data protection becomes a natural element of daily practice. As services become increasingly technology-driven, organisations must ensure that staff have the skills, structures, and support needed to handle personal data responsibly and to navigate new digital service models with confidence. Strengthening data protection competence is therefore not only a regulatory necessity but also a key factor in maintaining service quality, service user trust, and organisational resilience in a rapidly evolving digital environment.

1.3. Theoretical Framework

Overall, the theoretical perspectives presented in this chapter form a coherent foundation for examining how health and social care professionals understand and apply data protection requirements in their daily work. The legal and ethical frameworks of data protection, including the GDPR and sector-specific legislation, define the obligations that guide professionals' handling of sensitive service user information (Andreasson et al., 2023; Korpisaari et al., 2022).

At the same time, research on professional competence and digital capability highlights that compliance is not achieved through legislation alone, but through continuous learning, organisational support, and the ability to use digital systems securely and appropriately (Ministry of Social Affairs and Health, 2024b). These perspectives are particularly relevant in a sector where digitalisation progresses rapidly and where employees' readiness to use digital tools varies significantly. Finally, the

methodological principles of quantitative research provide the structure for analysing how these competencies manifest at the level of individual professionals, enabling systematic examination of variation in perceived understanding, training experiences, and support needs (Salkind, 2018; Vilkka, 2025).

Together, these strands form the analytical lens through which the empirical data of this thesis will be interpreted. They support the research question of the thesis: how well professionals feel they understand data protection requirements in their work, and how helpful they perceive current training tools to be. By integrating legal, organisational, and methodological perspectives, the framework enables a comprehensive analysis of the factors that shape data protection competence in contemporary health and social care services.

1.4. Hypothesis

A hypothesis is a clear and testable proposition or question about the relationship between variables. It is grounded in existing theories or previous empirical findings. Hypothesis can be theoretical, emerging from prior research, or empirical, based on the researcher's own observations and experiences. Testing a hypothesis requires operationalisation, meaning that abstract theoretical concepts are translated into measurable indicators. For example, variables such as age, gender, or job satisfaction must be defined and measured through structured questions or indicators. Without proper operationalisation, data analysis cannot be valid or reliable (Vilkka, 2021).

The hypothesis is based on the researcher's own observations and experiences in the social care field: respondents who have completed employer-provided data protection training are expected to rate their understanding of GDPR requirements higher than those who have not received such training.

The hypothesis guides the empirical analysis by clarifying the expected relationships between training, the perceived usefulness of learning tools, and data protection competence. It also provides a structured basis for interpreting the survey results in the following chapters.

Chapter 2 - Methodology

This chapter presents the methodological choices of the thesis and explains how the research was designed, implemented, and analysed. Its purpose is to provide a transparent and replicable account of how the data were collected and how the research question was addressed. The chapter begins by outlining the overall research design and approach, followed by a description of the data collection methods, participants, sampling strategy, and practical implementation. The analytical procedures for both quantitative and qualitative data are then detailed, together with an assessment of reliability, validity, and trustworthiness. Finally, the methodological choices are justified in relation to the research question, demonstrating the alignment between the thesis aims and its empirical execution.

To investigate health and social care professionals' perceptions, experiences, and training needs related to data protection, the thesis applies a mixed-methods survey design that combines quantitative and qualitative elements. A structured survey was used to gather data, enabling the examination of patterns, group differences, and competence levels across respondent groups. The research question focuses on professionals' understanding of data protection requirements, their evaluation of existing training tools, and the challenges they encounter when applying guidelines in practice.

To support the validity and interpretability of the findings, this chapter outlines the core methodological concepts that guide the thesis, including population and sampling strategies, variable types, data handling procedures, and the principles of reliability and validity. These foundations ensure that the analysis is robust and that the conclusions are relevant to the practical realities of data protection in professional settings.

2.1. Research Design

The thesis employed a mixed-methods survey design consisting of quantitative Likert-scale items and qualitative open-ended questions. The quantitative component enabled the systematic measurement of respondents perceived understanding of data protection requirements and the usefulness of current training tools. The qualitative items complemented this by allowing participants to elaborate on their experiences in their own words, thereby adding contextual depth to the numerical findings.

This design was appropriate for the research objectives, as a survey allows efficient data collection from a large and diverse group of health and social care professionals. Closed-ended items support reliable comparison across respondents, while open-ended questions capture nuances that may not emerge through quantitative measures alone. Together, these elements provide a comprehensive understanding of the phenomenon.

The aim of the thesis was to measure professionals perceived data protection competence and their experiences with current training tools. These objectives required collecting structured, comparable data from a larger group of respondents, which is best achieved through a quantitative survey. The design enables the identification of patterns, group differences, and associations between variables.

The overall design is grounded in a post-positivist research philosophy, which assumes that social phenomena can be measured, compared, and analysed using structured data. This approach is based on the idea that individuals' perceptions and experiences — such as their understanding of data protection requirements or the usefulness of training — can be transformed into measurable variables (see Annex B). The design also assumes that collecting data from a larger group of professionals enables the identification of general patterns and supports cautious generalisation of the findings.

Together, these methodological choices create a coherent chain from research questions to data collection and analysis.

2.2. Research Approach and Rationale

The thesis examines health and social care professionals perceived understanding of data protection requirements and their perceptions of the usefulness of the training tools they have used. It also explores the organisational context in which this competence is developed and applied.

The survey collected essential background information, including whether participants had completed employer-provided data protection training within the past three years, their years of experience in the field, their current work sector, and their professional role. These variables were selected because they directly support the examination of the research question and enable the testing of the thesis' hypotheses.

A structured and predetermined survey design supports the aims of the thesis by enabling the systematic measurement of constructs such as perceived competence and training usefulness. Closed-ended Likert-scale items allow for consistent comparison across respondents and provide quantifiable data suitable for statistical analysis. The qualitative questions allow respondents to explain, in their own words, why they perceive certain training tools as useful or not useful and to describe concrete challenges in their daily work.

An exploratory and interpretive component is needed because data protection competence is shaped not only by formal training but also by workplace culture, personal experiences, and contextual factors. These aspects are difficult to quantify but essential for understanding why professionals may feel confident or uncertain when applying data protection guidelines. The qualitative data therefore enrich the analysis by revealing nuances that structured items alone cannot capture.

2.3. Data Collection Methods

Data for the thesis were collected using an online survey. This method enables the efficient gathering of responses from a large and diverse group of health and social care professionals and allows participants to respond at a time and place convenient for them. The format also made it possible to distribute the questionnaire widely through social media channels, increasing the likelihood of reaching professionals across different sectors and countries.

The survey included both quantitative Likert-scale items and qualitative open-ended questions. The questionnaire used in this thesis is presented in Annex A. This combination allowed respondents to provide structured ratings while also elaborating on their experiences, opinions, and practical challenges. The mixed format strengthened the thesis by producing both comparable numerical data and contextual insights.

The survey also collected background information relevant to the research questions, such as work experience, training history, and professional role.

The questionnaire was developed through content validation, drawing on the theoretical framework of the thesis, including GDPR requirements, national data protection legislation, and previous research on data protection competence.

2.4. Participants and Sampling

In quantitative research, the statistical unit — or observation unit — refers to the object of analysis, such as a person, organisation, image, or text. The sample consists of a subset of these units, while the population (or base population) includes all the units from which information is desired. In many cases, studying the entire population is impractical due to limitations of time, cost, or accessibility. Therefore, researchers select a sample, which is a subset of the population chosen to represent the whole group (Salkind, 2018; Tähtinen et al., 2020; Valli, 2001, as cited in Vilkka, 2025).

A well-defined population and carefully constructed sample are essential prerequisites for the accuracy and credibility of quantitative research. To ensure representativeness, the characteristics and structure of the sample should correspond as closely as possible to those of the population. Proper sampling design helps minimise random variation and bias, thereby enhancing the validity of research results (Tähtinen et al., 2020).

In statistical notation, the entire population is usually denoted by a capital N, while the sample size is represented by a lowercase n. When sampling is not based on random selection, such as in convenience or purposive sampling, the study is said to rely on a sample population rather than a statistically defined population. The representativeness of the sample determines how well the findings can be generalised to the target population (Tähtinen et al., 2020).

Sampling can be carried out through various statistical sampling techniques. When the population cannot be precisely defined, non-probability or purposive sampling methods may be used instead. Proper planning of data collection and sampling ensures reliability and generalisability of results (Salkind, 2018; Tähtinen et al., 2020).

Heikkilä (2004, cited in Vilkka, 2025) emphasises that the larger the sample size, the more likely it is to capture the heterogeneity of the population. Heterogeneity refers to the degree of variation among observation units: a heterogeneous population has wide variability, while a homogeneous population has minimal variation. The actual sample refers to the number of valid responses obtained, and its adequacy must be assessed in relation to the entire population and the research objectives. Incomplete responses should only be included if they provide relevant and valid data (Vilkka, 2025). Valli (2018) notes that quantitative studies that are not based on probability sampling require more cautious interpretation, as their findings cannot be generalised in the same way.

The success of any research project largely depends on how participants are selected. Effective sampling strategies aim to ensure that the chosen group accurately represents the broader population, thereby improving the reliability and validity of research outcomes. To ensure equal participation opportunities, all potential respondents should have comparable access to technical tools, such as email or the internet. Survey methods are therefore well suited to populations consisting of professionals, employees, or young people with adequate digital access. When a sample fails to accurately represent the population, findings are restricted to the participants included and cannot be generalised (Salkind, 2018; Vilkka, 2025).

Together, these principles clarify how samples are formed and how findings can be interpreted in relation to the broader population. By defining the observation unit, outlining the sampling approach, and acknowledging the limits of representativeness, research establishes a transparent basis for assessing the generalisability and credibility of its results.

In this thesis the participants were volunteers reached primarily through social media and direct messages. Recruitment targeted individuals working in the health and social care sector who held a relevant professional degree, as these groups routinely handle service user data.

Inclusion criteria required participants to provide informed consent and to indicate that they worked in the health and social care sector. Those who had not completed employer-provided data protection training within the past three years were automatically excluded from training-related items.

The thesis applied a combination of purposive and convenience sampling. Purposive sampling ensured that the survey reached professionals who handle sensitive personal data as part of their daily work. Convenience sampling was used within this group, as participation was voluntary and based on accessibility through social media channels.

A total of N = 220 participants responded to the survey, of whom n = 156 (70.9%) completed the questionnaire in full.

2.5. Practical Implementation

The survey questions were designed based on the Ministry of Social Affairs and Health's Handbook: Promoting digitalisation and the related practices, competence and operating culture (2024b). While the Ministry's questionnaire targeted managerial roles, this thesis focused on professionals working directly with service users. Some thematic elements were adapted, but no items were copied directly.

The questionnaire was drafted in Excel in Finnish, Swedish, and English. Three native Finnish speakers, two native Swedish speakers, and one English teacher reviewed the language versions. Their feedback, together with comments from the thesis supervisor, was used to refine the items.

The survey was first tested on the EUSurvey platform, but technical limitations led to its implementation in Qualtrics. Before opening the survey, three individuals tested the flow and usability. The final version was published on 2 November 2025.

The survey was distributed widely through LinkedIn, Facebook, Instagram, Threads, WhatsApp groups, and direct messages. Posts on social media were published repeatedly during the three-week data collection period in Finnish, Swedish, and English. Participants were encouraged to share the link further.

Participation was voluntary, and no personal or identifying information was collected. Respondents were required to confirm that they had read and accepted the privacy notice before proceeding.

2.6. Data Analysis

Salkind (2018) states that precise variable definition, rigorous measurement, and careful attention to reliability and validity are essential for generating meaningful, generalisable conclusions in behavioural and social science research. As Vilkka (2021) explains, data analysis appears in the methodology and results sections. The process involves systematic examination, grouping, and interpretation of data to address the research question. The analysis aims to transform large sets of information into meaningful conclusions, thereby producing new knowledge related to the research

problem. The analytical process includes defining the research problem and hypotheses, determining what data is needed and how it will be collected, ensuring the data is sufficient and relevant to answer the research question, and systematically coding, categorising, and interpreting the content (Vilkka 2021).

Beyond sampling, researchers must also consider measurement levels. Variables are classified according to their measurement scale, which determines how data can be analysed statistically. Variables can be classified as nominal, ordinal, interval, or ratio. Nominal and ordinal scales are used for qualitative categorisation and ranking, while interval and ratio scales enable numerical comparison and statistical calculation. Attitude scales, such as Likert or Osgood semantic differential scales, measure opinions or attitudes (Salkind, 2018; Tähtinen et al., 2020; Vilkka, 2021).

Categorical variables describe qualitative characteristics that fall into distinct categories without inherent order. Because the categories are mutually exclusive and unordered, statistical summaries such as the mean or standard deviation are not meaningful. Instead, non-parametric methods and frequency distributions, such as cross-tabulations, are used to analyse categorical data (Tähtinen et al., 2020).

Salkind (2018) writes that in the behavioural and social sciences, most variables are measured at ordinal levels. Tähtinen et al. (2020) explain that ordinal variables represent data with a defined order but without equal intervals between categories. Attitude scales such as the five-point Likert scale are a typical example. Although ordinal data are strictly non-metric, researchers often treat them as approximately interval-scaled when composite variables are created, thereby allowing for parametric analysis. The decision to treat ordinal variables as interval-scaled depends on disciplinary conventions and methodological justification (Tähtinen et al., 2020; Vilkka, 2021).

Each observation, or data unit, is stored in a data matrix, where each row corresponds to a respondent and each column to a variable, such as gender, age, education, or employment status. Careful data entry is essential since input errors may cause measurement errors and reduce reliability. To minimise these, researchers may double-enter data or use software validation tools that flag inconsistencies (Alkula et al., 1995, as cited in Vilkka, 2021; Heikkilä, 2004, as cited in Vilkka, 2021).

Salkind (2018) explains that data coding is the process of transforming raw observations into a structured format suitable for analysis. Effective coding ensures that data are unambiguous and interpretable without losing their original meaning. Once coded, descriptive statistics are used to summarise data and provide an initial understanding of distributions (Salkind, 2018).

Valli (2018) explains that research findings may be presented in tables, figures, or key statistical values. Tables allow for the display of detailed information, whereas graphical figures provide an overview intended to simplify interpretation. Key figures, such as means, should be accompanied by appropriate measures of dispersion, such as standard deviation, to allow the reader to assess

variability (Valli, 2018). During the verification of quantitative data, it is crucial to detect potential errors, inconsistencies, or biases in the dataset. The analysis phase may reveal that the data is systematically skewed, for example when certain subgroups are under- or overrepresented. To address this issue, weighting is applied to ensure that the sample distribution reflects the characteristics of the total population (Alkula et al., 1995, as cited in Vilkka, 2021; Heikkilä, 2004, as cited in Vilkka, 2021). Valli (2018) points out that the key principle is to code data consistently and in a manner that supports later analysis.

Cross-tabulation examines how two or more categorical variables are related, showing whether one variable might influence another. However, such analysis does not prove causality, because similar patterns may appear by coincidence or due to an unmeasured third factor (Alkula et al., 1995, as cited in Vilkka, 2021; Heikkilä, 2004, as cited in Vilkka, 2021). The simplest example of cross-tabulation is a 2×2 table, which is clear but limited in detail. Larger tables may contain more information, but excessive categorisation can reduce clarity. When the number of observations is small, reporting both frequencies and percentages is recommended. In larger datasets, percentages are usually sufficient, though the explanatory variable should always be clearly identified (Valli, 2018).

By outlining the logic of cross-tabulation, the role of numerical coding, and the ethical requirements guiding data collection, this section clarifies the analytical framework used in the thesis. These principles help ensure that relationships between variables are examined systematically and that methodological choices remain aligned with established research standards. Such coherence strengthens the interpretive value of the findings and supports a transparent transition from methodological theory to the empirical analysis of data protection competence.

Through appropriate sampling, variable classification, and statistical testing, quantitative research seeks to ensure that findings derived from a sample can be generalised to the wider population with scientific accuracy and reliability. These measurement principles provide the foundation for selecting analytical techniques and interpreting the survey data. By understanding how variables are classified and how different scales guide statistical choices, the thesis ensures that its analyses remain consistent with methodological standards.

The data were analysed to understand how professionals perceive their data protection competence and how they have been trained in this area. The three-year timeframe for training was selected due to the 2023 wellbeing services county reform in Finland.

Quantitative data were analysed using descriptive statistics, including crosstabulations, percentages, modes, medians, and means. These methods were appropriate for describing respondent profiles and examining patterns in the Likert-scale items.

Qualitative data (see Annex C) were analysed using an inductive, data-driven approach. Open-ended responses were read multiple times, coded, and grouped into themes. Particular

attention was paid to ensuring consistent coding across the three language versions. Themes were named only after the groups had formed, ensuring an inductive process.

All variables and coding procedures are described in Annex B. The thematic coding categories are presented in Annex D. Rigour was ensured by repeated reading, systematic coding, and grounding all themes directly in participants' responses.

2.7. Reliability, Validity, and Trustworthiness

In quantitative research, reliability (consistency) and validity (accuracy) are crucial for assessing the trustworthiness of results. Reliability refers to the consistency or stability of measurements: a reliable instrument produces similar results under consistent conditions. Reliability may be examined by comparing responses to similar items using correlation coefficients. Validity concerns how well the measurements capture the intended concepts and whether an instrument measures what it is intended to measure. Both qualities are critical because unreliable or invalid measurements can lead researchers to incorrect conclusions (Salkind, 2018; Vilkka, 2021).

Reliability refers to the consistency of measurements — such as time, raters, or test forms — ensuring that repeated assessments under similar conditions produce comparable results. According to Heikkilä (2004, cited in Vilkka, 2025), reliability is demonstrated when repeated measurements yield identical outcomes and when findings are generalisable within their intended context. Research reliability is strengthened by accurate data collection, a representative sample, careful data entry, and minimising measurement errors. Larger samples tend to produce more stable results that better represent the target population. Researchers should transparently report any limitations or potential biases that may affect the study's credibility (Heikkilä, 2004, as cited in Vilkka, 2021; Nummenmaa, 2006, as cited in Vilkka, 2021; Salkind, 2018).

The reliability of a measurement is determined by the proportion of true score variance relative to error variance, with higher reliability indicating that observed scores closely approximate true values. Errors can stem from the measurement method or participant characteristics. Enhancing reliability can involve increasing the number of observations, clarifying ambiguous items, standardising procedures, and maintaining consistent scoring. Correlation coefficients quantify consistency, with higher correlations reflecting greater reliability (Salkind, 2018).

Alkula et al. (1995, as cited in Vilkka, 2021) explain that by combining variables, a researcher can assess whether variable combinations are logical and identify internal inconsistencies. Initial statistical summaries — such as percentages, means, and standard deviations — provide the first descriptive insights into the dataset, including measures of symmetry and normality. Random errors may still occur if respondents misremember details, interpret questions differently, or if researchers make recording

mistakes. Such errors should be acknowledged and analysed during interpretation (Vilkka, 2025). Nieminen (1991, as cited in Vilkka, 2025) notes that comparing inconsistencies with previous research can help identify potential errors and enhance credibility.

Ensuring validity involves careful conceptualisation of variables, precise instrument design, and thoughtful formulation of questions that accurately represent the research problem. Systematic errors, such as misinterpretation of questions, can compromise validity (Valli, 2001, as cited in Vilkka, 2025; Heikkilä, 2004, as cited in Vilkka, 2025; Hirsjärvi et al., 2005, as cited in Vilkka, 2025). Different types of validity include content validity, criterion validity, and construct validity (Salkind, 2018). Validity concerns whether the instrument measures what it intends to measure (Valli, 2001, as cited in Vilkka, 2025; Heikkilä, 2004, as cited in Vilkka, 2025; Hirsjärvi et al., 2005, as cited in Vilkka, 2025; Salkind, 2018).

In attitudinal or opinion surveys, structured response options such as Likert-type scales are commonly used. The placement of a category such as “I cannot say” is important when results are analysed beyond simple frequencies. For some respondents, this option may indicate genuine indecision rather than neutrality. Placing this option at the midpoint maintains validity and avoids distorting results. Quantitative studies that are not based on probability sampling require more cautious interpretation, as their findings cannot be generalised in the same way. Ensuring that relevant background variables are represented in the sample is essential (Valli, 2018).

Variables can also be classified as continuous or discrete. Continuous variables can assume any value along a spectrum, while discrete variables take distinct, mutually exclusive values. Precise definition of variables enhances interpretive power and generalisability. Measures of central tendency — mean, median, and mode — summarise distributions: the mean calculates the arithmetic average, the median identifies the midpoint, and the mode indicates the most frequent value (Salkind, 2018).

A clear understanding of reliability and validity strengthens the methodological foundation of this thesis and supports the interpretation of its findings. By examining how measurement consistency is ensured, how errors are minimised, and how well the survey items reflect underlying concepts, the research builds a transparent basis for evaluating the credibility of its results. This alignment between measurement quality, analytical choices, and the research questions enhances the trustworthiness of the conclusions drawn about data protection competence in health and social care work.

The questionnaire items were carefully checked for grammar and clarity. The Finnish, Swedish, and English versions were reviewed by native speakers and pilot-tested with four health and social care professionals. Minor adjustments were made based on feedback.

Validity was ensured through alignment with the theoretical framework, GDPR requirements, national legislation, and the Ministry’s 2024 handbook. The supervisor and volunteers reviewed all language versions, and each item was checked against the research question.

Qualitative data were coded systematically following the guidelines of the Finnish Social Science Data Archive. Themes and typifications are presented in the annexes B and D to support transparency.

The number of incomplete responses was unexpected and remains unexplained.

2.7.1 AI Use Disclosure

This thesis has made limited and ethically compliant use of the AI-assisted tool Microsoft Copilot, following the general rules and best practices of the institution. AI was not used as an author, nor was any AI-generated content presented as original research or cited as a source. All interpretations, analyses, and conclusions are entirely the researchers' own.

AI assistance was used only for permitted purposes, including brainstorming ideas, planning the thesis structure and headings, refining search keywords, and improving the clarity and language of text written by the researcher. Copilot also supported the technical accuracy of APA7 references, including spelling, formatting, and consistency in both in-text citations and the reference list. In addition, AI was used to suggest alternative wording to avoid unnecessary repetition and to provide guiding questions that helped place content under appropriate sections.

All AI-generated suggestions were critically evaluated before inclusion. No confidential, personal, or copyright-restricted material was entered into AI tools. The use of AI is openly disclosed here in accordance with academic integrity requirements.

2.8. Justification of Methodological Choices

The thesis required both quantitative and qualitative questions to address different aspects of the research questions. Likert-scale items enabled structured measurement, while open-ended questions allowed respondents to describe their experiences and reflections.

The selection of questions, scales, and languages was guided by the research questions and the anticipated respondent group. Finnish, Swedish, and English versions increased accessibility and ensured accurate interpretation of specialised terminology.

Purposive and convenience sampling ensured that the survey reached relevant professionals while enabling broad participation.

Qualtrics was selected due to its usability and built-in analytical tools. Pilot testing supported the reliability and clarity of the instrument. The chosen analytical methods were appropriate for describing the phenomenon and answering the research questions.

2.9. Alignment with Research Question

Each methodological step was designed to support answering the research question. The Likert-scale items aligned with the quantitative aspects of the thesis, while open-ended questions deepened understanding of the underlying factors.

The multilingual questionnaire ensured accurate interpretation of specialised terminology. Pilot testing strengthened clarity and relevance. Purposive sampling ensured that the survey reached professionals who handle service user data.

Descriptive statistics and thematic analysis were selected to match the nature of the data and the research question. The systematic coding and theme development ensured that qualitative findings were grounded in the data.

2.10. Analysis of Open-ended Responses

In addition to the structured survey data, this thesis includes open-ended responses that provide deeper insight into professionals' experiences, perceptions, and challenges related to data protection. These qualitative elements complement the quantitative findings by highlighting nuances that cannot be captured through predefined answer options. To analyse these responses systematically, three methodological approaches were applied: coding, thematic analysis, and typification. Together, these methods support the interpretation of professionals' training needs, perceived competence gaps, and suggestions for improving organisational practices.

2.10.1. Coding

Coding is a foundational phase of qualitative data analysis in which raw textual material is systematically organised into meaningful units. It involves reading the data closely and assigning short labels (codes) that capture the essence of specific ideas, expressions, or observations. These codes may describe actions, perceptions, challenges, or any other relevant aspect of the material. Coding serves two primary purposes: it reduces large volumes of text into manageable segments, and it creates an analytical structure that supports the identification of broader patterns (Finnish Social Science Data Archive, 2026a).

In this thesis, coding is used to organise open-ended survey responses so that recurring issues related to data protection competence, training experiences, and perceived challenges can be examined in a structured manner. Through this process, the data are condensed and arranged in a way that enables systematic pattern identification.

2.10.2. Thematic Analysis

Thematic analysis is an interpretive method used to identify, analyse, and report patterns (themes) within qualitative data. After the initial coding phase, related codes are grouped to form preliminary themes that represent shared meanings across the dataset. These themes are then reviewed, refined, and defined to ensure that they accurately reflect the content and nuances of the material (Finnish Social Science Data Archive, 2026b).

Thematic analysis is particularly suitable for open-ended survey responses because it enables the researcher to capture both common viewpoints and more subtle variations in participants' experiences (Finnish Social Science Data Archive, 2026b). In this thesis, thematic analysis is applied to explore how professionals describe their understanding of data protection requirements, the usefulness of current training tools, and the types of support they consider necessary in their daily work. Through this process, patterns of meaning within the coded data are identified and refined to ensure that the themes accurately represent the nuances of the responses.

2.10.3. Typification

Typification is a complementary analytical strategy in which individual responses are classified into broader categories or "types" based on shared characteristics. While thematic analysis focuses on identifying patterns of meaning, typification aims to construct representative categories that summarise typical ways of thinking, behaving, or experiencing a phenomenon. This approach is particularly useful when qualitative insights need to be aligned with a predominantly quantitative research design, as it enables the transformation of narrative responses into structured categories that can be compared across respondent groups (Finnish Social Science Data Archive, 2026c).

In this thesis, typification is used to group open-ended responses into meaningful types, such as common training needs, frequently mentioned challenges, or typical interpretations of data protection guidelines. Thereby supporting the integration of qualitative insights into the overall analysis.

2.11. Limitations

The use of convenience sampling limits the generalisability of the findings. Most respondents were from Finland, and the sample consisted predominantly of Bachelor of Social Services graduates, which may influence response patterns.

Self-report data may introduce bias, and the high number of incomplete responses raises questions about survey length or relevance. Minor interpretation differences between language versions are possible, and AI-assisted translation may introduce small inaccuracies. Although Qualtrics provided all necessary analytical functions, some advanced features may not have been available. In

addition, differences in education and work experience may influence the generalisability of the results.

The methodological choices in this thesis were selected to address the research question systematically. The mixed-methods survey enabled the collection of both structured quantitative data and rich qualitative insights, while the sampling strategy ensured participation from professionals directly involved in handling service user information. The analytical procedures were conducted transparently, and the steps taken to ensure reliability and validity support the credibility of the findings. Overall, the methodology provides a coherent and well-justified foundation for the empirical results presented in the next chapter.

Chapter 3 - Research Findings

This chapter presents the results of the thesis, combining both quantitative and qualitative data to answer the research questions. The findings are organised thematically to reflect the structure of the survey and the analytical focus of the thesis. Each section addresses the research question or analytical theme, beginning with background characteristics of the respondents and followed by their understanding of data protection requirements, perceptions of current training tools, and the integration of open-ended responses. The chapter concludes with a summary that synthesises the key insights and prepares the reader for the final conclusions and implications.

3.1. Introduction to the Research Findings

This chapter presents the empirical findings of the thesis. The results are reported descriptively and without interpretation, focusing on what the data reveal about professionals' perceptions of data protection competence and their experiences with training. To provide a clear structure, the findings are organised according to the research question guiding the thesis: How health and social care professionals understand and apply data protection requirements in their work, and how helpful do they find current training tools.

The quantitative results are reported using descriptive statistics, including frequencies, percentages, medians, and modes, as well as cross-tabulations that illustrate differences between respondent groups. These analyses provide an overview of the distribution of responses and highlight patterns relevant to the research question. The qualitative comments are used to support and deepen the understanding of these patterns by illustrating how respondents describe their experiences in their own words. To maintain analytical clarity, qualitative insights are presented alongside the relevant quantitative themes but are kept separate from interpretation, which is addressed in Chapter 4.

Together, these findings offer a comprehensive picture of how professionals perceive their own competence, how they experience current training practices, and what kinds of challenges or support needs they identify in their daily work.

3.2. Background Characteristics of Respondents

This section presents the key demographic and professional characteristics of the respondents. These variables are essential for interpreting the findings and for understanding how different groups of professionals perceive their data protection competence and training experiences. The background variables also form the basis for the cross-tabulations used later in this chapter.

3.2.1. Country of Employment

The majority of respondents are from Finland, representing 88% (n = 175) of the sample. The remaining participants were located in Portugal (7%, n = 13), Greece (3%, n = 5), Germany (2%, n = 3), and Italy and Sweden (1% each, n = 1). The strong representation of Finnish respondents reflects the researcher's professional networks and the distribution channels used during data collection.

3.2.2. Education and Profession

Respondents represented a range of health and social care professions. The largest group consisted of Bachelor of Social Services graduates (40%, n = 79). Registered nurses formed the second-largest group (22%, n = 44), followed by those who selected "Other" (18%, n = 36). Practical nurses accounted for 15% (n = 29), while doctors/physicians represented 4% (n = 7). Social workers (n = 2) and dentists (n = 1) each accounted for 1% of the sample. This distribution reflects the strong participation of social services professionals, which is consistent with the recruitment channels used.

3.2.3. Work Environment / Sector

Nearly half of the respondents worked in social services (48%, n = 95), followed by healthcare (35%, n = 69) and other sectors (17%, n = 34). It is important to note that in Finland, healthcare professionals such as practical nurses and registered nurses may also work in social services settings (e.g., housing units), and both health and social care professionals may work in NGOs. This overlap is relevant when interpreting sector-based comparisons.

3.2.4. Years of Experience

Respondents had varying levels of professional experience. More than half reported over ten years of experience (56%, n = 92). The remaining respondents had 2–5 years (21%, n = 35), 6–10 years (20%, n = 32), or less than two years of experience (3%, n = 5). The mean value for the experience variable was 3.29 (min = 1, max = 4, SD = 0.90, N = 220), indicating that the sample leaned toward highly experienced professionals.

3.2.5. Employment Sector

Most respondents worked in the public sector (73%, n = 144). The private sector accounted for 22% (n = 43), and NGOs or associations for 6% (n = 11). This distribution reflects the structure of the Finnish health and social care system, where public sector employment is common.

3.2.6. Participation in Employer-Provided Data Protection Training

Most respondents (79%, n = 157) reported having completed employer-provided data protection training within the past three years, while 21% (n = 41) had not. This variable is central to the thesis, as it determines which respondents were shown the training-related Likert-scale items.

3.2.7. Use of Background Variables in Cross-Tabulations

Several background variables were selected for cross-tabulations because they are directly relevant to the research question:

1. Work sector (social services, healthcare, other). These sectors differ in their statutory responsibilities, service user groups, and data protection practices. Comparing them helps identify whether perceived competence varies across service environments.
2. Years of experience. Experience may influence confidence and familiarity with data protection requirements. More experienced professionals may have encountered repeated training cycles or practical situations that strengthen competence.
3. Education/profession. Different professions have distinct legal obligations and training traditions. Cross-tabulations help determine whether certain professional groups perceive data protection differently.
4. Participation in employer-provided training. This variable is essential for comparing trained and untrained respondents and for examining whether training is associated with higher perceived competence.

These background characteristics provide the foundation for understanding group differences and interpreting the quantitative findings presented in the following sections.

3.3. Understanding of Data Protection Requirements

This section presents the findings related to how well do health and social care professionals feel they understand data protection requirements in their work. The results are based on selected survey items that most directly measure respondents perceived understanding of their responsibilities, their knowledge of key data protection concepts, and the extent to which data protection is embedded in everyday work practices.

The researcher selected six Likert-scale items for detailed examination because they provide the clearest insight into how professionals evaluate their own competence and how data protection is reflected in organisational routines. These items capture both individual-level understanding and the broader working culture surrounding data protection.

The following survey questions form the basis of the analysis:

1. Q22.1: “I understand my role and responsibilities in handling personal data in my work.” This question measures perceived clarity of professional responsibilities.
2. Q22.3: “I understand what the EU General Data Protection Regulation (GDPR) means in my day-to-day work.” This question assesses practical understanding of GDPR requirements.
3. Q24.1: “I systematically follow the data protection guidelines of my organisation in my work.” This question reflects the extent to which organisational rules are applied in practice.
4. Q24.4: “I know what special categories of personal data are.” This question measures conceptual knowledge of a core GDPR definition.
5. Q24.5: “I know how to process personal data correctly (e.g., electronically, on paper).” This question assesses practical procedural knowledge.
6. Q26.4: “Data protection issues are regularly discussed in my working unit.” This question indicates whether data protection is part of the organisational learning culture.

Together, these items provide a comprehensive view of perceived data protection competence. They cover both knowledge (e.g., GDPR, special categories), practical skills (e.g., correct processing), behaviour (e.g., following guidelines), and organisational context (e.g., discussion culture). The results of these items are presented in the following sections using descriptive statistics and cross-tabulations to highlight differences between respondent groups.

3.3.1. Self-assessed Understanding of Roles and Responsibilities (Q22.1)

Respondents who had participated in data protection training within the last three years reported very high levels of perceived understanding of their responsibilities. Among trained respondents, 86% selected strongly agree, and the mean score was 4.83 on a 5-point scale. Those without training also reported high understanding, with 72% selecting strongly agree and a mean score of 4.41. Overall, both groups expressed strong confidence, although trained respondents showed slightly higher average scores.

Across all experience groups, respondents reported high perceived understanding of their responsibilities. Strong agreement was the most common response in every category. The highest concentration of strong agreement was found among respondents with more than ten years of experience, but high understanding was also evident among those with fewer years in the field. Differences between experience groups were small.

3.3.2. Understanding of GDPR in Daily Work (Q22.3)

Respondents' perceived understanding of what the GDPR means in their day-to-day work was generally high. Among those who had completed data protection training within the last three years, most selected either partially agree or strongly agree, with a total of 107 respondents expressing agreement. Those without training also reported understanding GDPR reasonably well, although their responses were more evenly distributed across the scale and included slightly more disagreement. Overall, training did not appear to create a clear or substantial difference in perceived understanding, as both trained and untrained respondents reported relatively high confidence.

When examining the results by education and profession, the pattern remained similar. Across all professional groups (practical nurses, Bachelor of Social Services graduates, registered nurses, doctors, social workers, dentists, and those who selected "other") agreement was more common than disagreement. The largest professional groups, particularly Bachelor of Social Services graduates and registered nurses, showed strong concentrations of agreement. Smaller professional groups also indicated understanding, although their distributions were naturally more varied due to low respondent numbers. Overall, no profession-specific differences emerged that would clearly distinguish one group as having higher or lower perceived understanding of GDPR.

3.3.3. Practical Knowledge of Data Protection (Q24.1, Q24.4, Q24.5)

Respondents generally reported that they systematically follow the data protection guidelines of their organisation. Among those who had completed training, most selected either partially agree or strongly agree, with the majority falling into the latter category. Those without training also reported high levels of agreement, although their responses included slightly more disagreement and neutral answers. Overall, both groups indicated that they follow organisational guidelines, but a small number of respondents in each group selected disagreement, suggesting that not all professionals consistently adhere to data protection practices. The reasons for this cannot be determined from the survey data.

Although the survey data does not reveal the underlying reasons, the researcher's practical experience in social care suggests a few possible explanations. Differences in training quality, varying interpretations of data protection obligations, inconsistent organisational practices, and time pressures in daily work may all contribute to occasional non-compliance. In some cases, professionals may also lack up-to-date guidance or feel uncertain about how the GDPR requirements apply in complex service user situations. These factors could partly explain why a small number of respondents reported disagreement.

When examining the results by years of experience, strong agreement was again the most common response across all groups. Respondents with more than ten years of experience showed the

highest concentration of agreement, but even those with fewer years in the field reported following guidelines. Only a few respondents in the less experienced groups selected disagreement. Overall, experience appeared to correlate with higher confidence in following organisational guidelines, although agreement was common across all experience levels.

Respondents' knowledge of special categories of personal data showed more variation. While many participants agreed that they know what these categories are, both trained and untrained respondents included individuals who selected strongly disagree or partially disagree. This indicates a noticeable knowledge gap, particularly given that health and social care professionals routinely handle special categories of personal data in their work. Training did not eliminate this variation, and it is unclear whether the training content explicitly covered special categories.

Table 3.1 Distribution of responses to Q24.4. Source: Author's own work 2026.

Response option	Total (n=198)	Practical Nurse	Bachelor of Social Services	Registered Nurse	Dentist	Dental Hygienist	Social Worker	Physician	Other
Strongly disagree	14 (7.1%)	3 (10.3%)	5 (6.3%)	2 (4.5%)	0 (0%)	0 (0%)	0 (0%)	2 (28.6%)	2 (5.6%)
Partially disagree	26 (13.1%)	0 (0%)	11 (13.9%)	9 (20.5%)	0 (0%)	0 (0%)	1 (50.0%)	1 (14.3%)	4 (11.1%)
Neither agree nor disagree	13 (6.6%)	2 (6.9%)	4 (5.1%)	5 (11.4%)	0 (0%)	0 (0%)	0 (0%)	1 (14.3%)	1 (2.8%)
Partially agree	50 (25.3%)	8 (27.6%)	21 (26.6%)	11 (25.0%)	0 (0%)	0 (0%)	0 (0%)	1 (14.3%)	9 (25.0%)
Strongly agree	95 (48.0%)	16 (34.5%)	38 (48.1%)	17 (38.6%)	1 (100%)	0 (0%)	1 (50.0%)	2 (28.6%)	20 (55.6%)

As shown in Table 3.1, respondents' knowledge of special categories of personal data varied across educational backgrounds. While most selected 'strongly agree', uncertainty and disagreement were present in all major professional groups.

Experience-based differences were also visible. Respondents with more than ten years of experience showed the highest levels of agreement, but disagreement and uncertainty were present in every experience group. When examined by education, the largest professional groups (practical nurses, Bachelor of Social Services graduates, and registered nurses) showed similar patterns:

agreement was common, but each group included respondents who did not recognise what special categories of personal data are. This suggests that the knowledge gap is not limited to a single profession.

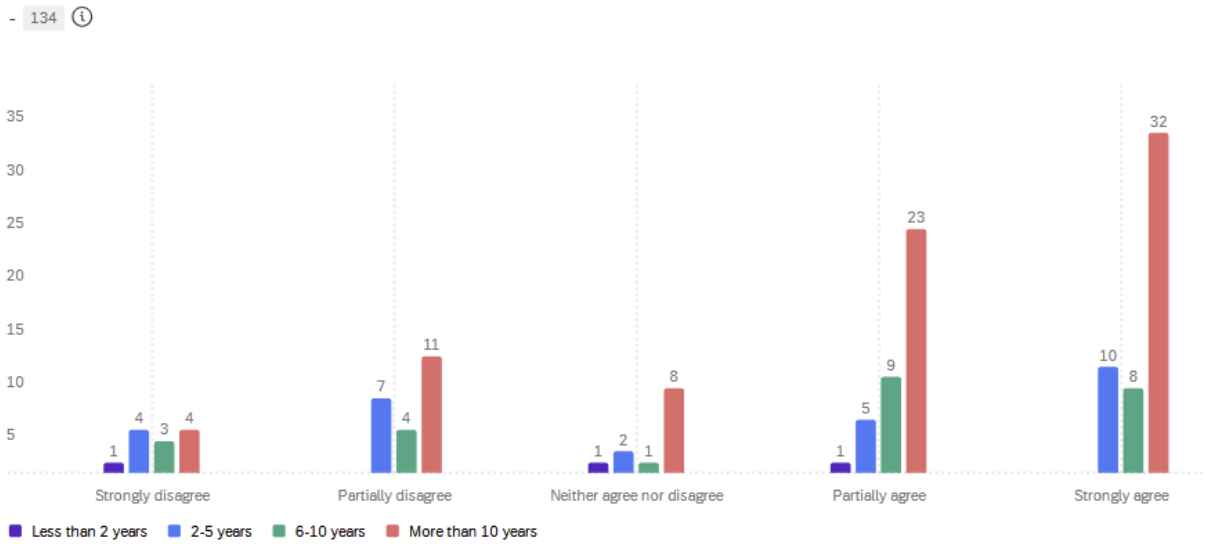


Figure 3.1 Respondents' agreement levels on correct processing of personal data, grouped by years of experience. Source: Author's own work 2026.

Respondents' perceived ability to process personal data correctly was generally high, as shown in Figure 3.1. Those who had completed training reported strong confidence, with the majority selecting strongly agree. Untrained respondents also expressed confidence, although their responses were more evenly distributed and included a few disagreement options. Across experience groups, agreement was consistently high, and in the 6–10-year group no respondents selected disagreement at all. Respondents with more than ten years of experience again showed the highest concentration of strong agreement.

3.3.4. Organisational Context: Discussion of Data Protection in the Work Unit (Q26.4)

Respondents' views on whether data protection issues are regularly discussed in their working unit varied across sectors. As illustrated in Figure 3.2, disagreement was more common than agreement in social services, with a notable proportion selecting either strongly disagree or partially disagree. Healthcare respondents showed an even stronger pattern of disagreement, indicating that regular discussion of data protection is not widely experienced in these environments. Among those working in other sectors, the distribution between agreement and disagreement was more balanced, with no clear majority in either direction.

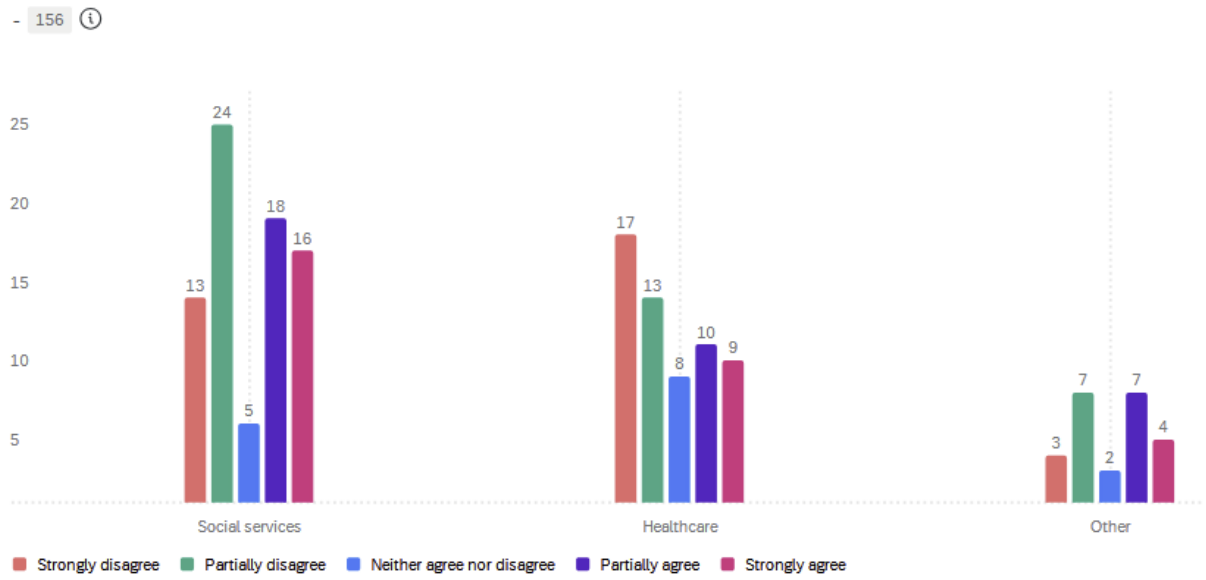


Figure 3.2 Respondents' agreement levels on whether data protection issues are regularly discussed in their unit, by sector. Source: Author's own work 2026.

Neither the quantitative nor qualitative data provided information on how often such discussions take place, only whether respondents perceive them as occurring regularly. The overall pattern suggests that discussions about data protection are not consistently embedded in everyday work practices across sectors. The higher levels of disagreement in healthcare, and to a lesser extent in social services, may indicate a lack of organisational routines or expectations regarding when and how data protection issues should be addressed. It is also possible that professionals do not always recognise situations that would warrant discussion or do not feel encouraged to raise such issues within their teams.

3.3.5. Summary of Findings for Understanding of Data Protection Requirements

Overall, the results indicate that respondents perceive their understanding of data protection requirements as high across multiple dimensions. Most participants felt very confident about their responsibilities, and strong agreement was the dominant response in items related to understanding

GDPR, following organisational guidelines, and processing personal data correctly. Although trained respondents generally reported slightly higher levels of understanding and practical competence, untrained respondents also expressed high confidence, and the differences between the groups were modest. This means that researcher's first hypothesis was only partially supported: training was associated with somewhat higher ratings, but the effect was not strong or consistent across all items.

Experience-based differences were also limited. Respondents with more than ten years of experience tended to report the highest levels of confidence, but high agreement was common across all experience groups. Professional background did not appear to strongly influence perceived understanding, as the main professional groups showed similar response patterns.

A notable finding was the clear variation in respondents' knowledge of special categories of personal data. Despite working in environments where such data are routinely handled, disagreement and uncertainty were present in every group, including among those who had completed training. Another unexpected observation was that regular discussion of data protection issues was not widely reported in any sector, suggesting that organisational routines for addressing data protection may not be firmly established. Taken together, the results show that while respondents feel confident in many aspects of data protection, certain conceptual areas and workplace practices reveal gaps that warrant further attention.

3.4. Helpfulness of Current Training Tools

This section addresses how do professionals perceive the clarity and usefulness of current training tools related to data protection. The analysis focuses on respondents' experiences with onboarding materials, e-learning modules, employer-provided courses, and other forms of organisational training. The results highlight which formats are considered most helpful, where gaps exist, and how training practices align with professionals' everyday responsibilities. Both quantitative ratings and qualitative comments are used to illustrate the strengths and limitations of current approaches.

3.4.1. Perceived Clarity of Training Materials (Q19.3)

This question was displayed only to respondents who indicated that they had completed data protection training. For this reason, Qualtrics did not generate any "no" responses for this item, as untrained respondents were not shown the question at all. The results therefore represent only the perceptions of those who had participated in training.

Q19_3 - The training materials provided by the organisation (e.g. instructions, e-learning courses) are clear and easy to understand.

Field	Min	Max	Mean	Median	Standard Deviation	Variance	Responses	Sum
The training materials provided by the organisation (e.g. instructions, e-learning courses) are clear and easy to understand.	1.00	5.00	3.86	4.00	1.07	1.15	140	541.00

Figure 3.3 Descriptive statistics for respondents' ratings of the clarity and ease of understanding of training materials (Q19_3). Source: Author's own work 2026.

As shown in the statistical summary (Figure 3.3), the training materials were generally perceived as clear and easy to understand. The mean score was 3.86 (SD = 1.07), with a median of 4.00, indicating that most respondents agreed with the statement, although some variation was present.

Respondents who had completed data protection training generally perceived their organisation's training materials as clear and easy to understand. Most selected either partially agree or strongly agree, although a small number expressed disagreement or uncertainty. Because this item was only shown to respondents who had completed training, the results reflect the views of those with direct experience of the materials, and none of the respondents selected a complete lack of clarity.

When examined by work environment, the pattern was broadly similar across sectors. In social services, agreement was more common than disagreement, although a noticeable minority selected partially disagree. Healthcare respondents also tended to agree that the materials were clear, but their responses included slightly more disagreement than in social services. Among respondents working in other sectors, agreement was again the dominant pattern, with only a few selecting disagreement or neutral options. Across all environments, the majority of respondents perceived the materials as at least somewhat clear.

3.4.2. Perceived Impact of Training on Skills (Q19.2)

This question was displayed only to respondents who indicated that they had completed data protection training. For this reason, Qualtrics did not generate any “no” responses for this item, as untrained respondents were not shown the question at all. The results therefore represent only the perceptions of those who had participated in training.

Respondents who had completed data protection training expressed mixed views on whether the organisation’s trainings had increased their skills. Most respondents selected either partially agree or strongly agree, indicating that many felt the training had been beneficial. At the same time, a notable number chose partially disagree or strongly disagree, suggesting that the perceived impact of training was not uniform across participants. Neutral responses were also present, reflecting uncertainty or difficulty in assessing the effect of training.

Because this item was only shown to respondents who had completed training, it is not possible to compare trained and untrained groups. The results therefore reflect only the experiences of those who had direct exposure to the organisation’s training materials. Overall, the findings suggest that while many respondents felt that training had improved their skills, a meaningful minority did not perceive a clear benefit.

Despite having completed training, respondents still showed uncertainty regarding special categories of personal data, suggesting that current training may not fully address this conceptual area.

3.4.3. Importance of Practical Exercises (Q19.6)

This question was displayed only to respondents who indicated that they had completed data protection training. For this reason, Qualtrics did not generate any “no” responses for this item, as untrained respondents were not shown the question at all. The results therefore represent only the perceptions of those who had participated in training.

Respondents generally considered practical exercises, such as case examples or simulations, important for learning data protection. Across all experience groups, agreement was more common than disagreement, although the strength of agreement varied. Respondents with more than ten years of experience showed the highest concentration of partially agree and strongly agree responses, suggesting that experienced professionals may place slightly more emphasis on the value of practical exercises. Those with fewer years of experience also tended to view practical exercises positively, although their responses were somewhat more dispersed across the scale.

When examined by work environment, the pattern remained consistent. In social services, agreement was clearly dominant, with a large proportion selecting strongly agree. Healthcare respondents also valued practical exercises, though their responses included a small number of

disagreement options. Among respondents working in other sectors, agreement was again the most common response, with very few selecting disagreement. Overall, the results indicate broad support for the idea that practical, scenario-based learning methods are beneficial for understanding data protection.

These quantitative findings align with the qualitative comments, where several respondents explicitly mentioned that simulations, case examples, or concrete scenarios would help them better understand data protection requirements. Together, the results suggest that practical exercises are widely perceived as a useful component of data protection training across different professional backgrounds and experience levels.

3.4.4. Experience and Perceived Need for Further Training

The bar chart in the Figure 3.4 illustrates the relationship between respondents' years of work experience in the health or social care sector and their perceived need for further education on data protection. A total of 117 responses is categorised into four experience groups: Less than 2 years, 2–5 years, 6–10 years, and More than 10 years. Within each group, responses are segmented by level of agreement, ranging from Strongly disagree to Strongly agree.

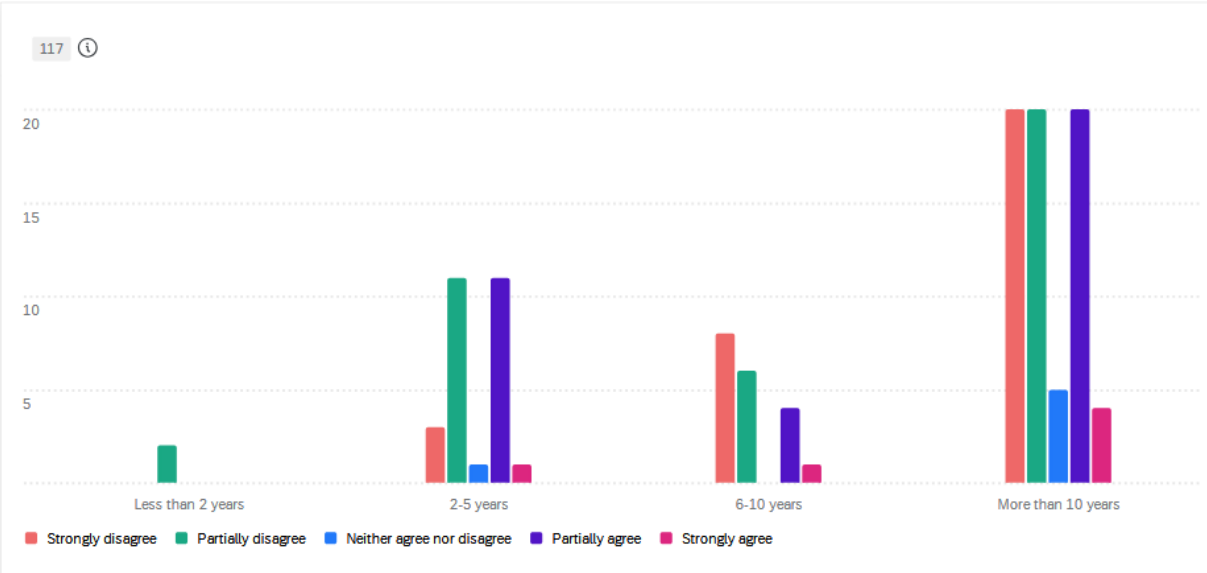


Figure 3.4 Respondents' agreement on the need for further data protection training, grouped by years of experience. Source: Author's own work 2026.

The group with more than 10 years of experience demonstrates the highest overall response volume, with responses distributed fairly evenly across disagreement, neutrality, and partial agreement. Strongly agree responses are present but not dominant. Respondents with less than 2 years of experience show very limited representation, with all responses falling into the agreement categories. The intermediate experience groups (2–5 years and 6–10 years) display mixed patterns,

with Partially disagree, Neither agree nor disagree, and Partially agree appearing most frequently depending on the group.

This figure highlights that perceptions of the need for further data protection training vary across experience levels, without a single dominant trend. The results suggest that respondents at all career stages express differing views on the necessity of additional education, indicating that training needs may be influenced by factors beyond tenure alone.

3.4.5. Summary of Findings for Helpfulness of Current Training Tools

Overall, respondents who had completed data protection training generally perceived the training materials as clear, and this pattern was similar across different work environments. Views on whether the training increased competence were more varied: many respondents felt that their skills had improved, while others did not report a clear benefit. This indicates that the training was mostly viewed positively, although its perceived impact was not fully consistent. Respondents who had completed training tended to rate their competence slightly higher than those without training, but the differences were small. As a result, researcher's first hypothesis received only partial support, as training appeared to enhance competence to some extent but not strongly or uniformly.

A notable finding was that uncertainty remained regarding special categories of personal data, even among respondents who had completed training. This suggests that education alone did not eliminate knowledge gaps in this area. In contrast, practical exercises were widely valued: nearly all respondents considered case examples or simulations important for learning data protection, and this view was shared by both experienced and less experienced professionals. Qualitative comments reinforced this, as participants explicitly expressed a need for concrete, scenario-based learning methods.

Experience showed a modest association with perceived competence, with more experienced respondents reporting slightly higher confidence. However, the differences were not large, and less experienced respondents also felt capable. This suggests that competence may not stem solely from experience or formal training, but also from organisational practices and the routines of individual work units. Sector differences were small overall. Health and social care respondents showed slightly more uncertainty about the usefulness of training, while the "other" group reported more consistent views. These patterns may reflect differences in how training is implemented across organisational contexts.

This pattern was also reflected in the experience-based diagram, where respondents with longer work histories more frequently recognised the need for continued training, although the differences between experience groups remained modest.

Taken together, the results show that while training materials are generally considered clear and practical exercises are strongly valued, the overall impact of training on competence is moderate, and certain conceptual areas, particularly special categories of personal data, remain challenging across sectors and experience levels.

3.5. Integration of Quantitative and Qualitative Findings

The qualitative comments presented in Annex C largely supported the quantitative findings. The importance of practical exercises was evident in both datasets: almost all respondents agreed quantitatively that hands-on training is essential, and the qualitative comments reinforced this by explicitly requesting case examples, simulations, and concrete, real-world scenarios that reflect situations professionals encounter. In this respect, the two data sources clearly pointed in the same direction.

The perceived benefit of training showed more variation in the quantitative results, and the qualitative material helped explain why. Respondents described that training practices were not consistent across the organisations, some workplaces did not engage in any discussion about data protection, and several participants felt that the materials were unclear or too general. Others mentioned a lack of support from supervisors. These factors help clarify why the training did not increase competence as strongly as might have been expected.

Quantitatively, respondents with more experience reported slightly higher levels of competence. The qualitative findings supported this pattern by showing that experience brings a sense of confidence. However, even the most experienced professionals expressed a continued need for practical exercises, indicating that experience alone is not sufficient. Across both datasets, organisational culture emerged as a more influential factor than either experience or training. This helps explain why the differences between experience groups remained relatively small.

3.6. Overall Summary of Findings

Most participants considered their data protection competence to be reasonably good. However, special categories of personal data emerged as the clearest knowledge gap. While professional experience contributed to a certain level of confidence, its effect was modest. Instead, organisational practices appeared to have a stronger influence on professionals' competence than experience alone.

Training materials were generally perceived as clear, yet the perceived benefit of training was inconsistent and not uniform across respondents. Importantly, the training did not eliminate uncertainty regarding special categories of personal data. Across both datasets, practical exercises stood out as the most desired and valued learning method.

Organisational culture played a central role in shaping competence. The qualitative comments highlighted issues such as a lack of discussion within work units, unclear instructions, and varying practices across teams. These factors help explain the variation observed in the quantitative results.

Synthesising the findings from the research question, the overall level of competence can be described as adequate but not comprehensive. Training contributed to competence only partially, whereas practical, hands-on methods emerged as the most important area for development. Ultimately, organisational culture and the everyday practices of work units appear to be the key elements in maintaining and strengthening data protection competence.

Conclusions

The final chapter summarises the main findings of the thesis, answers the research question, and discusses their practical implications. It also reflects on the strengths and limitations of the research and offers recommendations for future development of data protection competence in health and social care settings. The chapter concludes by identifying areas for further research and suggesting how organisations can better support professionals in meeting data protection obligations.

Answers to the Research Question

The findings showed that most participants felt they had sufficient knowledge of data protection to perform their work tasks and understood the overall meaning and importance of data protection. Strong agreement was the dominant response in items related to understanding GDPR principles, following organisational guidelines, and processing personal data correctly. Although respondents who had completed training generally reported slightly higher levels of understanding and practical competence, untrained respondents also expressed high confidence. The differences between the groups were modest, indicating that the researcher's hypothesis was only partially supported: training was associated with somewhat higher competence ratings, but the effect was neither strong nor consistent across all items.

Training was generally perceived as clear and understandable, but respondents expressed a strong desire for more practical learning methods, such as simulations and case-based exercises. Across different work environments, trained respondents consistently viewed the training materials as clear. However, perceptions of whether the training increased competence varied: many participants felt that their skills had improved, while others did not experience a clear benefit. This suggests that training was viewed positively overall, but its impact was not uniform. Respondents who had completed training tended to rate their competence slightly higher than those without training, yet the differences remained small.

The results align closely with the aims outlined in the thesis proposal. The thesis provides a broad overview to the research question of how professionals perceive their data protection competence, how sufficient they consider current training methods, and what kinds of support they find valuable. The findings offer practical insights for improving training design, updating internal policies, and strengthening organisational strategies related to data protection.

Practical Implications

The thesis also sheds light on whether current employer-provided measures, such as signing off on reading data protection plans or completing self-paced online courses, are perceived as sufficient in practice. The results suggest that while these measures provide a foundation, they may not fully meet professionals' needs, particularly in situations requiring applied judgement. The findings highlight the importance of support, onboarding, and practical training methods that help professionals feel confident and competent in real-life work situations. This is especially relevant in the fast-paced health and social care sector, where independent reading may be difficult to prioritise and may not translate directly into applied competence.

The findings indicate that while data protection training is available and generally considered clear, its practical effectiveness is limited. In practice, this means that organisations cannot rely solely on online, self-paced courses or mandatory click-through modules to ensure competence. Training should incorporate real-life situations, scenario-based exercises, and opportunities for discussion with colleagues or other participants. These elements help professionals translate abstract rules into concrete actions, which is essential in the complex and fast-paced environment of health and social care work.

The results also show that mandatory training is often completed quickly and with minimal engagement, which reduces its impact. When training becomes a routine requirement rather than a meaningful learning experience, professionals may not acquire new knowledge or deepen their understanding. This is particularly problematic in areas such as special categories of personal data, where uncertainty remained even among trained respondents.

A key practical implication is that competence does not develop solely through formal training or experience, but through everyday organisational practices. Without systematic follow-up, supervision, or shared discussions within work units, data protection routines may drift over time. This increases the risk that issues are only noticed when a breach occurs. Organisations should therefore recognise that maintaining data protection competence requires ongoing support, clear guidance, and a culture where data protection is actively discussed rather than treated as an administrative obligation.

Overall, the most important real-world insight is that effective data protection competence is built through practical, context-specific learning and strong organisational culture, not through isolated online modules alone.

Strengths and Limitations

The sample of 220 respondents provides a broad overview of experiences across different sectors, work environments, and educational backgrounds. While the sample is not statistically representative of the entire health and social care workforce, it is sufficiently diverse to offer meaningful insights into professionals' perceptions. The three-week data collection period allowed responses to accumulate steadily, and the topic itself was timely and relevant to daily work. The three language options increased accessibility, enabling participation from individuals beyond the researcher's personal networks. The online format also made it possible for many respondents to participate efficiently and simultaneously.

Despite these strengths, several limitations must be acknowledged. One limitation relates to the scope of the survey questions. While respondents reported high levels of understanding regarding data protection requirements, the survey may not have fully captured whether they can apply this knowledge in practice or whether certain aspects of data protection are misunderstood or overlooked. This raises the possibility that some participants may perceive themselves as competent even if their practical implementation does not fully align with legal or organisational expectations.

The thesis was also influenced by contextual factors. Majority of the participants were based in Finland, and a large proportion worked in social services or held a Bachelor of Social Services degree. These characteristics may shape how data protection is understood and practiced, and they limit the generalisability of the findings to other countries or professional groups.

Some questions could not be fully answered. The thesis did not reveal why many respondents struggled to recognise special categories of personal data, nor did it clarify why some participants did not complete the survey. More importantly, the findings suggest that even when training is completed, certain data protection practices may still not be implemented consistently in daily work. The reasons behind this gap, whether related to organisational culture, workload, unclear instructions, or other factors.

Recommendations

The findings highlight several areas where organisations, training developers, and managers can strengthen data protection competence in practice. First, work units should be required to discuss data protection at regular intervals. Structured conversations, such as monthly team discussions, theme weeks, or short briefings, would help keep data protection visible in everyday work. These sessions could be supported by the organisation's data protection officer, who could share anonymised examples of recent issues or breaches and clarify how similar situations should be handled.

Training developers should place greater emphasis on practical, scenario-based learning. Instead of relying primarily on online modules that can be completed quickly with limited engagement, training should incorporate real cases, simulations, and examples drawn from actual work situations. Using visual materials such as photographs, short videos, or gamified exercises based on real organisational environments (for instance offices, housing units, kitchens, clinics, corridors) may help participants recognise familiar contexts and better understand how data protection principles apply in their own work.

Managers and supervisors also play a crucial role. Strengthening their training would enable them to guide staff more effectively and ensure that data protection practices are consistently implemented in service user work. Supervisors should be equipped to model correct practices, address uncertainties, and integrate data protection into routine supervision and onboarding.

At the organisational level, data protection should be treated not only as a mandatory requirement but as an ongoing, shared responsibility. This requires systematic follow-up, clear communication, and a culture where data protection is actively discussed rather than assumed. By combining practical training, regular dialogue, and strong managerial support, organisations can create conditions where data protection competence is maintained and strengthened across all professional groups.

Future Research

Several questions remain unanswered and offer valuable directions for future research. One important area concerns the limited understanding of special categories of personal data. Although many respondents had completed training, uncertainty persisted. Future studies could explore why this knowledge gap remains: for example, whether special categories are insufficiently emphasised in training, whether the terminology is unfamiliar, or whether the concept is difficult to apply in practice.

Qualitative approaches such as interviews or focus groups would be particularly useful for examining how professionals interpret and implement data protection in real-life situations. Observational studies could provide even deeper insight by identifying practices that may not align with organisational guidelines or legal requirements. Such research would require a willing organisation but could offer highly valuable information about how data protection is enacted in everyday work and where gaps between training and practice emerge.

Further research could also investigate how data protection training can be made more effective, especially given that the topic can be both abstract (legal principles) and concrete (physical handling of documents or devices). Studies could examine the impact of scenario-based learning, simulations, or other practical methods on competence development. Gamification may also be a promising

avenue, particularly for professionals with experience in digital learning environments or for interdisciplinary teams combining social care, healthcare, and information technology perspectives.

Overall, future research should focus on understanding how data protection knowledge is internalised, how training can better support applied competence, and how organisational culture shapes everyday practices. Such studies would build on the present findings and contribute to developing more effective, context-sensitive approaches to data protection training and implementation.

The overall message of the thesis is that while data protection training is widely available, it does not automatically translate into higher competence or deeper understanding. Participants generally felt confident in their abilities, yet the findings show that current training formats, which were often based on self-paced online modules, do not significantly enhance knowledge on their own. Respondents clearly expressed a desire for more practical, scenario-based training that reflects real work situations.

The key takeaway about data protection competence is that it develops gradually through experience, but the effect of experience is modest. Even seasoned professionals reported uncertainties in specific areas, particularly regarding special categories of personal data. This indicates that competence is not solely a function of years in the field but depends on how well organisations support learning and reinforce correct practices.

The key takeaway about training is that clarity alone is not enough. Although training materials were generally considered understandable, their impact on competence was inconsistent. Effective training must go beyond information delivery and include concrete examples, simulations, and opportunities for discussion. Practical learning methods are essential for helping professionals apply data protection principles in everyday work.

Finally, the key takeaway about organisational culture is that it plays a decisive role. Competence is shaped not only by individual knowledge but by the routines, expectations, and conversations within work units. Organisations should pay closer attention to the content and structure of training, encourage regular team discussions about data protection, and create an environment where data protection is actively integrated into daily practice rather than treated as a one-time requirement.

Bibliographic References and Sources

Act on Health Care Professionals (559/1994). (1994). Finlex. https://www.finlex.fi/fi/laki/ajantasa/1994/19940559

Act on Social Welfare Professionals (817/2015). (2015). Finlex. https://www.finlex.fi/fi/laki/ajantasa/2015/20150817

Addis, C., & Kutar, M. (2018). The general data protection regulation (GDPR), emerging technologies and UK organisations: Awareness, implementation and readiness. Salford Business School. https://salford-repository.worktribe.com/output/1341709/

Andreasson, A., Oravala, J., & Toivonen, M. (2023). Tietosuoja ja yksityisyys: Opas jokaiselle [Data protection and privacy: A guide for everyone]. Tietosanoma.

Andreasson, A., Ylipartanen, A. (2025). Osaava tietosuojavastaava: Tietosuojatyön haasteet ja ratkaisut [Competent data protection officer: Challenges and solutions in data protection work] (3rd ed.). Tietosanoma.

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations. *Computer Science & IT Research Journal, 5(3)*, 528–543. https://doi.org/10.51594/csitrj.v5i3.859

Berisha, A.-K., Hakalisto, L., Heikkinen, P., Helminen, J., Jaatinen, M., Judén, R., Kotomäki, K., Leppänen, P., Råback, M., & Tulkki, H. (2025). Target state of digitalisation in liberal adult education (Publications of the Ministry of Education and Culture 2025:10). Ministry of Education and Culture. https://urn.fi/URN:ISBN:978-952-415-224-2

Chapple, M. (2024). CC℠ certified in cybersecurity: Study guide. Sybex, a Wiley Brand.

Constitution of Finland (731/1999). (1999). Finlex. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Data Protection Act (1050/2018). (2018). Finlex. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union, 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Finnish Government. (2020). Competence secures the future: Parliamentary policy approaches for reforming continuous learning (Publications of the Finnish Government 2020:38). Finnish Government. https://urn.fi/URN:ISBN:978-952-383-610-5

Finnish Social Science Data Archive. (2026a). Koodaaminen [Coding]. Retrieved January 30, 2026, from https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/koodaaminen/

Finnish Social Science Data Archive. (2026b). Teemoittelu [Thematic analysis]. Retrieved January 30, 2026, from https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/teemoittelu/

Finnish Social Science Data Archive. (2026c). Tyypittely [Typification]. Retrieved January 30, 2026, from https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/tyypittely/

Helminen, J. (2021). Jatkuvan oppimisen koulutukset ja osaamisen kehittämistarpeet sosiaalialalla [Continuing education and competence development needs in social services] (Diak Työelämä 23). Diakonia University of Applied Sciences. https://urn.fi/URN:ISBN:978-952-493-384-1

Holvikivi, J., & Lintula, L. (2022). Robotiikka- ja digitalisaatio-osaaminen asiakas- ja potilastyössä [Robotics and digitalisation competence in client and patient work]. In M. Elomaa-Krapu & A. Vuorijärvi (Eds.), *Osallistavia ratkaisuja digitaalisiin hyvinvointi- ja terveyspalveluihin* [Participatory solutions for digital welfare and health services] (pp. 26–36). Metropolia University of Applied Sciences. https://www.theseus.fi/bitstream/handle/10024/752859/2022%20Taito%2095%20Osallistavia%20ratkaisuja.pdf?sequence=2&isAllowed=y

Kambala, G. (2024). Data privacy in cloud computing: A comparative study of privacy preserving techniques. *International Journal of Scientific Research and Management, 12(6)*, 1299–1316. https://ijsrm.net/index.php/ijsrm/article/view/5372

Keller, M. (2023). Mitä on tietosuoja? [What is data protection?] Alma Talent.

Korpisaari, P., Pitkänen, O., & Warma-Lehtinen, E. (2022). Tietosuoja [Data protection] (2nd ed.). Alma Talent.

Lindström, A., Murto, L., & Uuskallio, A. (2025). Asiakastietojen käsittely sosiaali- ja terveydenhuollossa [Processing of client and patient data in health and social care]. Edilex Lakitieto Oy.

Lyly-Yrjänäinen, M. (2025). *Työolobarometri 2024* [Working conditions barometer 2024] (Publications of the Ministry of Economic Affairs and Employment 2025:21). Ministry of Economic Affairs and Employment. https://-686-4urn.fi/URN:ISBN:978-952-327-686-4

Ministry of Education and Culture. (2019). Development of studies leading to a qualification in support of the health and social services reform (Publications of the Ministry of

Education and Culture 2019:24). Ministry of Education and Culture. https://urn.fi/URN:ISBN:978-952-263-650-8

Ministry of Social Affairs and Health. (2024a). Competence required for the integration of healthcare and social welfare (Reports and Memorandums 2024:2). Ministry of Social Affairs and Health. https://urn.fi/URN:ISBN:978-952-00-5412-0

Ministry of Social Affairs and Health. (2024b). Handbook: Promoting digitalisation and the related practices, competence and operating culture (Publications 2024:37). Ministry of Social Affairs and Health. https://urn.fi/URN:ISBN:978-952-00-8657-2

Office of the Data Protection Ombudsman. (2026). Home. Retrieved January 30, 2026, from https://tietosuoja.fi/

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34(4)*, 757–778. https://doi.org/10.2307/25750704

Salkind, N. J. (2018). Exploring research (9th ed., Global ed.). Pearson.

Sorvettula, J. (2015). Tietosuoja [Data protection]. *FinJeHeW, 7(1)*, 36–43. https://journal.fi/finjehew/article/view/49622/14727

Tähtinen, J., Laakkonen, E., & Broberg, M. (2020). Tilastollisen aineiston käsittelyn ja tulkinnan perusteita [Basics of processing and interpreting statistical data] (2nd ed.). University of Turku.

Vilkka, H. (2021). Näin onnistut opinnäytetyössä [How to succeed in your thesis]. PS-kustannus.

Vilkka, H. (2025). Tutki ja kehitä [Research and develop] (6th ed.). Santalahti.

Voutilainen, T., & Kurvinen, E. (2024). Asiakas- ja potilastietojen käsittelyn sääntely [Regulation of client and patient data processing]. Alma Insights.

Yuan, B., & Li, J. (2019). The policy effect of the general data protection regulation (GDPR) on the digital public health sector. *International Journal of Environmental Research and Public Health, 16(6)*, 1070. https://doi.org/10.3390/ijerph16061070

Annexes

Annex A Survey Questionnaire on Social and Healthcare Professionals' Experiences and Training Needs

Q1 Information about the study

You are invited to participate in a survey conducted as part of a thesis project within the ManagiDiTH program. The purpose of this study is to explore social and healthcare professionals' experiences and training needs related to data protection. The survey is completely anonymous, and no personal data will be collected. Participation is voluntary, and you may discontinue your participation at any time. Survey responses will be treated confidentially, and individual respondents cannot be identified from the results. The results will be used in the thesis project, conducted in collaboration with ISCTE – Instituto Universitário de Lisboa, Laurea University of Applied Sciences, and Aristotle University of Thessaloniki. By proceeding to the survey, you consent to participate in this study.

Q1 Tietoa tutkimuksesta

Olet osallistumassa opinnäytetyönä tehtävään kyselyyn, joka on osa ManagiDiTH-opintokokonaisuutta. Tutkimuksen tarkoituksena on selvittää sosiaali- ja terveydenhuollon ammattilaisten kokemuksia ja koulutustarpeita tietosuojaan liittyen. Kysely on täysin anonyymi, eikä siinä kerätä mitään henkilötietoja. Osallistuminen on vapaaehtoista ja voit keskeyttää vastaamisen milloin tahansa. Kyselyn vastaukset käsitellään luottamuksellisesti, eikä yksittäisiä vastaajia voi tunnistaa tuloksista. Kyselyn tuloksia käytetään opinnäytetyössä, joka tehdään yhteistyössä ISCTE – Instituto Universitário de Lisboa, Laurea-ammattikorkeakoulun ja Aristotle University of Thessalonikin kanssa. Jatkamalla kyselyyn hyväksyt osallistumisesi tähän tutkimukseen.

Q1 Information om undersökningen

Du deltar i en enkät som genomförs som en del av ett examensarbete inom ManagiDiTH-programmet. Syftet med undersökningen är att utreda social- och hälsovårdspersonalens erfarenheter och behov av utbildning gällande dataskydd. Enkäten är helt anonym och inga personuppgifter samlas in. Deltagandet är frivilligt och du kan avbryta svarandet när som helst. Enkätens svar behandlas konfidentiellt och enskilda respondenter kan inte identifieras utifrån resultaten. Resultaten används i examensarbetet, som genomförs i samarbete med ISCTE – Instituto Universitário de Lisboa, Laurea

University of Applied Sciences och Aristotle University of Thessaloniki. Genom att fortsätta till enkäten godkänner du ditt deltagande i denna undersökning.

Q3 I have read and accept the attached privacy notice. Privacy notice.pdf

Yes

Q3 Olen lukenut liitteenä olevan tietosuojaselosteen ja hyväksyn sen. Tietosuojaseloste.pdf

Kyllä

Q3 Jag har tagit del av den bifogade dataskyddsbeskrivningen och godkänner den. Dataskyddsbeskrivning.pdf

Ja

Maa Which country do you work in?

▼ Afghanistan (1) ... Zimbabwe (1357)

Maa Missä maassa työskentelet?

▼ Afghanistan (1) ... Zimbabwe (1357)

Maa Vilket land arbetar du i?

▼ Afghanistan (1) ... Zimbabwe (1357)

Q19 Education

1. Practical nurse
2. Bachelor of Social Services (socionom)
3. Registered nurse
4. Dentist
5. Dental hygienist
6. Social worker
7. Doctor / Physician
8. Other

Q19 Koulutustaustasi

1. Lähihoitaja
2. Sosionomi
3. Sairaanhoitaja
4. Hammaslääkäri
5. Suuhygienisti
6. Sosiaalityöntekijä
7. Lääkäri

8. Muu

Q19 Välj utbildning i ditt nuvarande jobb om du har mer än ett jobb.

1. Närvårdare
2. Socionom
3. Sjukskötare
4. Tandläkare
5. Tandhygienist
6. Socialarbetare
7. Läkare
8. Annan

Q14 Work environment

1. Social services
2. Healthcare
3. Other

Q14 Toimintaympäristösi

1. Sosiaalihuolto
2. Terveydenhuolto
3. Muu

Q14 Verksamhetsmiljö

1. Socialvård
2. Hälso- och sjukvård
3. Annan

Display this question:

If Q14 = 1

Or Q14 = 2

Q15 Years of work experience in the social or healthcare sector

1. Less than 2 years
2. 2-5 years
3. 6-10 years
4. More than 10 years

Q15 Työkokemusvuotesi sosiaali- ja terveysalalla

1. Alle 2 vuotta
2. 2–5 vuotta

3. 6–10 vuotta
4. Yli 10 vuotta

Q15 Arbetslivserfarenhet inom social- och hälsovårdssektorn

1. Under 2 år
2. 2–5 år
3. 6–10 år
4. Över 10 år

Q16 Where do you work?

1. Public sector
2. Private sector
3. Non-governmental organisation (NGO) / association

Q16 Missä työskentelet?

1. Julkinen sektori
2. Yksityinen sektori
3. Kolmas sektori

Q16 Var arbetar du?

1. Offentlig sektor
2. Privat sektor
3. Tredje sektorn

Q18 Have you participated in a training on data protection in the last three years?

1. Yes
2. No

Q18 Oletko osallistunut tietosuojaa käsittelevään koulutukseen viimeisten kolmen vuoden aikana?

1. Kyllä
2. Ei

Q18 Har du deltagit i en utbildning om dataskydd under de senaste tre åren?

1. Ja
2. Nej

Display this question:

If Q18 = 1

Q19 Training and skills

The Likert scale: Strongly disagree (1); Partially disagree (2); Neither agree nor disagree (3); Partially agree (4); Strongly agree (5)

1) I need further training on data protection.
2) The organisation's trainings on data protection have increased my skills.
3) The training materials provided by the organisation (e.g. instructions, e-learning courses) are clear and easy to understand.
4) The organisation's trainings on data protection have been implemented in a way that is appropriate to me.
5) The trainings I have attended support my daily work and decision-making in data protection matters.
6) Practical exercises (case exercises or simulations) are important for the learning of data protection.
7) I have received sufficient practical guidance regarding data protection issues.

Q19 Koulutus ja osaaminen

Likert-asteikko: Täysin eri mieltä (1); Osittain eri mieltä (2); Ei samaa eikä eri mieltä (3); Osittain samaa mieltä (4); Täysin samaa mieltä (5)

1) Tarvitsen lisää koulutusta tietosuojaan liittyen.
2) Organisaation tarjoamat tietosuojakoulutukset ovat lisänneet osaamistani.
3) Organisaation tarjoamat koulutusmateriaalit (mm. ohjeet, verkkokurssit) ovat selkeitä ja helposti ymmärrettäviä.
4) Organisaation tarjoamat tietosuojakoulutukset on toteutettu minulle soveltuvalla tavalla
5) Käymäni tietosuojakoulutukset tukevat arjen työskentelyä ja päätöksentekoa tietosuoja-asioissa.
6) Käytännönläheiset harjoitukset (case-harjoitukset tai simulaatiot) ovat tärkeitä tietosuojan oppimisessa.
7) Olen saanut riittävästi käytännön ohjausta tietosuojakysymyksissä.

Q19 Utblidning och kompetens

Likertskalan nivåer: Instämmer inte alls (1); Instämmer delvis (2); Varken eller (3); Instämmer till stor del (4); Instämmer helt (5)

1) Jag behöver mer utbildning i dataskydd.
2) Organisationens erbjudna dataskyddsutbildningar har ökat min kompetens.
3) Organisationens utbildningsmaterial (till exempel anvisningar, nätkurser) är tydliga och lätta att förstå.
4) Organisationens dataskyddsutbildningar har genomförts på ett sätt som passar mig.
5) De utbildningar jag deltagit i stöder mitt dagliga arbete och beslutsfattande i dataskyddsfrågor.

6) Praktiska övningar (fallövningar eller simuleringar) är viktiga för att lära sig dataskydd.
7) Jag har fått tillräcklig praktisk handledning i dataskyddsfrågor.

Open-ended question:

Q20 What kind of training and in what format would you like to receive regarding data protection?

Q20 Millaista ja miten toteutettua koulutusta toivot tietosuojaan liittyen?

Q20 Vilken typ av utbildning och genomförandeform skulle du önska gällande dataskydd?

Open-ended question:

Q21 What type of training would you best fit to learn concrete data protection situations?

Q21 Millainen koulutusmuoto sopisi sinulle parhaiten käytännön tietosuojatilanteiden oppimista varten?

Q21 Vilken typ av utbildning är bäst lämpad för att lära dig konkreta dataskyddssituationer?

Q22 Awareness and understanding of data protection

The Likert scale: Strongly disagree (1); Partially disagree (2); Neither agree nor disagree (3); Partially agree (4); Strongly agree (5)

1) I understand my role and responsibilities in handling personal data in my work.
2) I am familiar with data protection policies and guidelines of my organisation.
3) I understand what the EU General Data Protection Regulation (GDPR) means in my day-to-day work.
4) I know when to report a data breach.
5) I feel that I have sufficient knowledge about clients'/patients' data protection rights.

Q22 Tietoisuus ja ymmärrys tietosuojasta

Likert-asteikko: Täysin eri mieltä (1); Osittain eri mieltä (2); Ei samaa eikä eri mieltä (3); Osittain samaa mieltä (4); Täysin samaa mieltä (5)

1) Ymmärrän roolini ja vastuuni henkilötietojen käsittelyssä omassa työssäni.
2) Tunnen organisaation tietosuojakäytännöt ja ohjeet.
3) Ymmärrän, mitä EU:n tietosuoja-asetus (GDPR) tarkoittaa omassa työssäni.
4) Tiedän, milloin on ilmoitettava tietosuojaloukkauksesta.
5) Minulla on riittävästi tietoa asiakkaiden/potilaiden tietosuojaan liittyvistä oikeuksista.

Q22 Medvetenhet och förståelse för dataskydd

Likertskalan nivåer: Instämmer inte alls (1); Instämmer delvis (2); Varken eller (3); Instämmer till stor del (4); Instämmer helt (5)

1) Jag förstår min roll och mitt ansvar när det gäller hantering av personuppgifter i mitt arbete.
2) Jag känner till organisationens dataskyddspraxis och riktlinjer.
3) Jag förstår vad EU:s dataskyddsförordning (GDPR) innebär i praktiken i mitt arbete.
4) Jag vet när en säkerhetsincident ska rapporteras.
5) Jag har tillräcklig kunskap om kunders/patienternas rättigheter rörande dataskydd.

Open-ended question:

Q23 What kind of information do you feel you need more of?

Q23 Millaista tietoa liittyen tietosuojaan koet tarvitsevasi lisää?

Q23 Vilken information anser du att du behöver mer av?

Q24 Data protection compliance in the organisation and in practical work

The Likert scale: Strongly disagree (1); Partially disagree (2); Neither agree nor disagree (3); Partially agree (4); Strongly agree (5)

1) I systematically follow data protection guidelines of my organisation in my work.
2) Following data protection guidelines at my workplace is easy and clear.
3) Personal data will be processed securely in my work unit.
4) I know what special categories of personal data are.
5) I know how to process personal data correctly (e.g. electronically, on paper).
6) I know who I can ask for help on data protection issues.
7) I am able to advise clients/patients on data protection matters.

Q24 Tietosuojan noudattaminen organisaatiossa ja käytännön työssä

Likert-asteikko: Täysin eri mieltä (1); Osittain eri mieltä (2); Ei samaa eikä eri mieltä (3); Osittain samaa mieltä (4); Täysin samaa mieltä (5)

1) Noudatan työssäni organisaation tietosuojaohjeita systemaattisesti.
2) Työpaikallani tietosuojaohjeiden noudattaminen on helppoa ja selkeää.
3) Henkilötietoja käsitellään työyksikössäni turvallisesti.
4) Tiedän, mitä erityiset henkilötietoryhmät ovat.
5) Tiedän, miten käsitellä henkilötietoja oikein (esim. sähköisesti ja paperilla).
6) Tiedän, keneltä voin kysyä tietosuojakysymyksissä apua.
7) Pystyn ohjeistamaan asiakkaita/potilaita tietosuojaan liittyvissä asioissa.

Q24 Efterlevnad av dataskyddsbestämmelser inom organisationen och i det dagliga arbetet

Likertskalan nivåer: Instämmer inte alls (1); Instämmer delvis (2); Varken eller (3); Instämmer till stor del (4); Instämmer helt (5)

1) Jag följer organisationens dataskyddsriktlinjer systematiskt i mitt arbete.

2) På min arbetsplats är det enkelt och tydligt att följa dataskyddsriktlinjerna.
3) Personuppgifter hanteras på ett säkert sätt i min arbetsenhet.
4) Jag vet vad särskilda kategorier av personuppgifter är.
5) Jag vet hur man hanterar särskilda personuppgifter på rätt sätt (till exempel elektroniskt och på papper).
6) Jag vet vem jag kan fråga om dataskyddsfrågor.
7) Jag kan ge vägledning till kunder/patienter om dataskyddsfrågor.

Open ended-question

Q25 What kind of practical changes or needs have you identified in your work unit in relation to data protection?

Q25 Millaisia käytännön muutoksia tai muutostarpeita olet havainnut työyksikössäsi liittyen tietosuojaan?

Q25 Vilka praktiska förändringar eller förbättringsbehov har du observerat i din arbetsenhet gällande dataskydd?

Q26 Risk management and reporting

The Likert scale: Strongly disagree (1); Partially disagree (2); Neither agree nor disagree (3); Partially agree (4); Strongly agree (5)

1) My organisation responds effectively to potential data protection risks.
2) The reporting of data breaches is easy and clear.
3) Information systems in which I process customer/patient data are secure.
4) Data protection issues are regularly discussed in my working unit.
5) I have the opportunity to contribute to the development of data protection issues in my workplace.

Q26 Riskienhallinta ja raportointi

Likert-asteikko: Täysin eri mieltä (1); Osittain eri mieltä (2); Ei samaa eikä eri mieltä (3); Osittain samaa mieltä (4); Täysin samaa mieltä (5)

1) Organisaationi reagoi tehokkaasti mahdollisiin tietosuojaan liittyviin riskeihin.
2) Tietosuojaloukkauksista raportoiminen on helppoa ja selkeää.
3) Tietojärjestelmät, joissa käsittelen asiakas- ja potilastietoja, ovat turvallisia.
4) Työyksikössäni keskustellaan säännöllisesti tietosuojakysymyksistä.
5) Minulla on mahdollisuus vaikuttaa tietosuoja-asioiden kehittämiseen työpaikallani.

Q26 Riskhantering och rapportering

Likertskalan nivåer: Instämmer inte alls (1); Instämmer delvis (2); Varken eller (3); Instämmer till stor del (4); Instämmer helt (5)

1) Organisationen reagerar effektivt på möjliga risker relaterade till dataskydd.
2) Det är enkelt och tydligt att rapportera dataskyddsbrott.
3) De informationssystem där jag hanterar kund- eller patientuppgifter är säkra.
4) I min arbetsenhet diskuteras dataskyddsfrågor regelbundet.
5) Jag har möjlighet att påverka utvecklingen av dataskyddsfrågor på min arbetsplats.

Open-ended question:

Q27 In general, briefly describe which data protection issues have been addressed in your work unit recently.

Q27 Kuvaile yleisluontoisesti, millaisia tietosuoja-asioita työyksikössäsi on lähiaikoina käsitelty.

Q27 Beskriv övergripande vilka dataskyddsfrågor som har behandlats i din arbetsenhet nyligen.

Annex B Coding Scheme / Variable List

1. Background Variables

COUNTRY

Coding: 1–1357 (Qualtrics country list)

Description: Country of employment

EDU

Coding:

1 = Practical nurse

2 = Bachelor of Social Services

3 = Registered nurse

4 = Dentist

5 = Dental hygienist

6 = Social worker

7 = Doctor/Physician

8 = Other

Description: Educational background

WORK_EXP

Coding:

1 = Less than 2 years

2 = 2–5 years

3 = 6–10 years

4 = More than 10 years

Description: Work experience in the social or healthcare sector

SECTOR

Coding:

1 = Public sector

2 = Private sector

3 = NGO/Association

Description: Employer sector

TRAINING_3Y

Coding: 0 = No, 1 = Yes

Description: Participation in data protection training in the past 3 years

PRIVACY_NOTICE_ACCEPTED

Coding: 0 = No, 1 = Yes

Description: Acceptance of privacy notice

2. Likert Scale Items (1 = Strongly disagree … 5 = Strongly agree)

A. Training and Skills (Q19)

TS1 – I need further training on data protection.

TS2 – The organisation's trainings on data protection have increased my skills.

TS3 – The training materials provided by the organisation are clear and easy to understand.

TS4 – The organisation's trainings have been implemented in a way that is appropriate to me.

TS5 – The trainings I have attended support my daily work and decision-making.

TS6 – Practical exercises (case exercises or simulations) are important for learning data protection.

TS7 – I have received sufficient practical guidance regarding data protection issues.

B. Awareness and Understanding (Q22)

AU1 – I understand my role and responsibilities in handling personal data.

AU2 – I am familiar with my organisation's data protection policies and guidelines.

AU3 – I understand what the GDPR means in my day-to-day work.

AU4 – I know when to report a data breach.

AU5 – I have sufficient knowledge about clients'/patients' data protection rights.

C. Compliance in Organisation and Practical Work (Q24)

CO1 – I systematically follow data protection guidelines in my work.

CO2 – Following data protection guidelines at my workplace is easy and clear.

CO3 – Personal data is processed securely in my work unit.

CO4 – I know what special categories of personal data are.

CO5 – I know how to process personal data correctly (electronically and on paper).

CO6 – I know who I can ask for help on data protection issues.

CO7 – I am able to advise clients/patients on data protection matters.

D. Risk Management and Reporting (Q26)

RM1 – My organisation responds effectively to potential data protection risks.

RM2 – Reporting data breaches is easy and clear.

RM3 – The information systems I use are secure.

RM4 – Data protection issues are regularly discussed in my work unit.

RM5 – I have the opportunity to contribute to the development of data protection issues.

3. Composite Variables (Summated Scales)

SUM_TS – Mean of TS1–TS7 (Training and skills)

SUM_AU – Mean of AU1–AU5 (Awareness and understanding)

SUM_CO – Mean of CO1–CO7 (Compliance in organisation and practical work)

SUM_RM – Mean of RM1–RM5 (Risk management and reporting)

Cronbach's alpha values will be reported in the results section.

4. Open-Ended Questions and Coding Themes

Q20 – Preferred type and format of training

T20_1 – Practical examples

T20_2 – Clearer materials

T20_3 – In-person training

T20_4 – Online training

T20_5 – Unit-specific training

T20_6 – Regular training

Coding: 0 = not mentioned, 1 = mentioned

Q21 – Best format for learning practical data protection situations

T21_1 – Simulations

T21_2 – Workshops

T21_3 – Case examples

T21_4 – Online modules

T21_5 – Peer learning

Q23 – Information needs

T23_1 – GDPR principles

T23_2 – Practical procedures

T23_3 – Data breach reporting

T23_4 – Rights of clients/patients

T23_5 – Special categories of personal data

Q25 – Practical changes or needs in the work unit

T25_1 – Improved instructions

T25_2 – Better systems

T25_3 – More training

T25_4 – Improved processes

T25_5 – Communication needs

Q27 – Recent data protection topics addressed in the work unit

T27_1 – Data breaches

T27_2 – Guidelines

T27_3 – System changes

T27_4 – Rights of clients/patients

T27_5 – Risk management

5. Variable Naming Conventions

Background variables: COUNTRY, EDU, WORK_EXP, SECTOR, TRAINING_3Y

Training & skills: TS1–TS7

Awareness & understanding: AU1–AU5

Compliance: CO1–CO7

Risk management: RM1–RM5

Composite variables: SUM_TS, SUM_AU, SUM_CO, SUM_RM

Open-ended codes: T20_x, T21_x, T23_x, T25_x, T27_x

Annex C Qualitative Responses

Q20: What kind of training and in what format would you like to receive regarding data protection?

Kaikille toimintaympäristössä työskenteleville ammattiryhmille yhteistä konkreettiseen toimintaan sovellettavaa sekä kaikilla ammattiryhmässä työskelevien äidinkielellä tarjottavaa koulutusta, jossa huomioidaan myös työntekijän tietosuoja. Tällä hetkellä asiakaan ja työntekijän tietosuojaohjeistus ovat erillisiä, työntekijän tietosuojatiedon jäädessä vähäiselle huomiolle.

Webinars, Presentations, written material and guide with FAQs presenting scenarios, interactive e-learning courses.

Selkeää, joka ei jätä niin paljoa yksittäisen työntekijän harkinnan varaan. Esim. "Asiakastietojärjestelmästä saa katsoa vain palvelun kannalta olennaiset tiedot" on hyvin subjektiiviseen kokemukseen perustuva

Itsenäisesti, netissä tehtävä. Esim medieco learn tai oppiportti.

Toivoisin koulutusta tietosuoja-asetuksen (Gdpr:n sisällöstä) keskeisestä sisällöstä.

Lisäksi toivoisin koulutusta henkilötietojen käsittelyyn liittyvistä riskeistä ja miten riskejä voidaan hallita.

Toivoisin, että koulutus olisi toteutettu esimerkiksi Teamsillä ja että koulutuksessa olisi käytännön läheisiä esimerkkejä.

Vapaaehtoista

Hybrid training course, combination of online and in person

Kerrottais selkeästi asiat tilannesidonnaisesti

Verkkokurssi, jossa paljon esimrkkejä ja aitoja tilanteita, jotka jäävät mieleen. Kurssille voisi myös tarvittaessa palata tarkistamaan asioita eikä niin, että tentin suoritettua se menee kiinni.

Verkkokoulutus omaan tahtiin toteutettavana. Yleiset GDPR jutut, ilmoittautumiset, palautteet, tietojen säilyttäminen jne.

Verkkokoulutus on ihan toimiva. Toki luento aiheesta esim. koulutuspäivillä voisi olla toimiva tapa kerrata asioita.

Esimerkkejä

Ajankohtaista, työpaikan toimintoihin liittyvää, semmoista mihin helppo palata etsimään vastauksia jos joku mietityttää

Continous training once a year would be very helpful. Some things get forgotten, some new issues are coming out that I would like to learn about and being updated.

Netti käy hyvin.

Case- harjoituksia toivoisin. Käytännön asioita.

Any kind really, anything is better than nothing that so far has been provided

Ylläpitokoulutusta toki, mutta tekoälyn ja digitalisaation lisääntyessä niihin liittyvää lisäkoulutusta.

Omaan toimintaympäristöön räätälöityä koulutusta. Ei ns ”liukuhihnalla” koulutusta.

Lainsäädäntö, soveltaminen tietosuojakäytäntöihin

Tietosuoja kysymykset opiskeluhuollon kontekstissa

Mitä on kiellettyä ja sallittua

e learning sessions

Fysiska kurser

Lisää käytäntöä. Lähiopetus olisi kiinnostava, koska pakolliset verkkokurssit käydään läpi nopeasti, jolloin niistä ei jää paljoa käteen.

Luentomuotoisesti toteutettua koulutusta tietosuojan juridiikasta.

Se opetettiin koulussa ja hyvin opetettiinkin.

Ongelmia on tuottanut vain tartuntatauti laki, joka estää työntekemisen.

Toivoisin, että koko henkilöstö olisi ymmärtänyt tietosuojakysymykset hallintia myöten, ettei rivistä pitäiai huomautella että jossakin asiassa tietosuoja on hatara

Konkreettisia esimerkkejä arjen työstä.

Lyhyt ytimekäs

Selkeää, konkreettista ja sellaista, joka ymmärtää toimintakentän

Muutakin kuin kirjaukseen liittyvää

Tarkemmin esim. gdpr

Pakolliset verkkokurssit vaikeasti ymmärrettävällä kielellä, puuduttavan pitkiä, niihin ei anneta tarpeeksi aikaa. Nopea workshop jossa olisi käytännön tilanteita omaan työyksikköön ajatellen olisi paljon parempi

Digital format, with specific examples from my day-to-day activities.

Verkkokurssit ja mahdollisesti myös asiantuntijan vetämään syvällisempää koulutusta

En osaa sanoa, mutta yleisesti tietosuojakoulutukset eivät ole kauhean kiinnostavia.

Verkkokursseja

Scenario with real people example, interactive and workshop to evaluate assimilation.

Juuri omaan työympäristön ja työtehtäviin kytkeytynyttä tietosuojakoulutusta.

Tietoturvauhkien tunnistaminen

Lastensuojeluun kohdennettua tietosuojakoulutusta.

Nykyään koulutukset netissä ja tentti lopussa jota saa yrittää niin monta kertaa että läpi menee. Kuka sellaisesta oppii? Eikä näihin anneta aikaa eikä hiljaista tilaa jotta voisi oikeasti ajatuksen kanssa lukea ja koittaa oppia

Case-tyyppistä, mahdollisimman arjen tasolle vietynä.

Small interactive pratical sessions with content about data protection

Workshop

Keskustelu livenä.

Säännöllistä, että pysyy aihe pinnalla. Verkkokoulutukset olen kokenut hyvänä sekä tilaisuudet joissa on voinut asiantuntijalta saada vastauksia ihan käytännöstä nousseisiin asioihin.

Digital training

Enemmän käytännön asioihin liittyvää

Full training

Esimerkkejä,miten jossain tilanteessa toimitaan

Konkreettisempaa ja käytännönläheisempää.

Säännöllistä, ja aina kun tulee jotain uutta.

I don't know enough about types and formats of training to reply.

Verkkokursseja ja case ratkaisuja

Verkkopohjaista eri oppimisalustoilla. Mutta myös käytännön stimulaatioita esim poistumisharjoituksen pitämiseen.

Lyhyisiin clippeihin jaetut koulutusvideot, muutama minuutti/video

Säännöllisiä, ajankohtaisista tietoturva ilmiöistä/uhkista kertovia koulutuksia.

Live koulutus jossa voisi kysyä tarkentavia kysymyksiä.

Toivoisin koulutusta, joka olisi räätälöity juuri meille. Koulutus olisi hyvä tapahtua yksikön tiloissa, jotta kouluttaja ymmärtäisi ympäristön jossa työskennellään. Alan ymmärrys olisi tärkeää.

Käytännönläheisempää

Omaan ammattialaan liittyvää kohdennettua koulutusta

Koulutusta, jossa käytäisiin läpi käytännön tasoa sellaisella kielellä, että sen ymmärtää tavallinen työntekijä. Jos ei ole tekniikan tai hallinnon parissa töissä voi joitain koulutuksia olla vaikeaa ymmärtää. Tarpeeksi pienelle ryhmälle kerrallaan, jotta kysyminen ja tarkentaminen on mahdollista. Myöskin vastauksia niihin tilanteisiin kun tietosuoja ja käytäntö ovat räikeässä ristiriidassa.

Käytännön viemistä omaan työhön esimerkein.

Etäkoulutuksia, vaikka edes kerran vuodessa pakollisesti

Verkkokurssi ja simulaatiot

Mahdollisimman yksinkertaista sekä kompaktia

Helposti saatavilla olevaa, kaikille pakollista ja sopivalla aikavälillä kerrattavaa/ uusittavaa

Puolipäivää kestäviä luentoja.

Verkkokurssit

Alaan liittyvää yksityiskohtaista tietoa

Verkossa toteutettava koulutus on riittävä.

Luentojen ja case-työskentelyn yhdistelmiä, etätoteutus tavoittaa laajemmin mutta livekoulutuksessa on etunsa, mikäli kouluttaja on innostava
Continuous information security and protection online training every six months
Enemmän käytännön asioita
I don't know
Isossa organisaatiossa (hva), jossa tietosuoja koulutus on kaikille sama, olet sitten hammashoitaja tai sosiaalityön johtaja, tietosuojakoulutus on liian ylätasoinen ja ns. helppo, jottai se konkreettisesti turvaisi tietosuojaosaamisen.
Nyt tuntuu, että se tehdään vain tekemisen vuoksi. Tai, että paperilla näyttää, että henkilöstö koulutettu.
Käytännön case-esimerkkejä. Tipsejä. Verkkokoulutus.
Koulutusta ei ole ollut. Sen sijaan olen suorittanut jonkinlaisen "Tietosuojapassin", jossa kyseltiin GDPR-säädöksiä.
Case tyyppiset asiat, oikeaan elämään liittyvät asiat
Tietosuojan keskeiset riskit ja sitä tukevaa juridisuutta.
Esimerkit ovat hyviä ja silmiä avaavia.
Jotain muuta, kuin power point esityksiä.
Konkreettista ohjetta, jossa mahdollisimman vähän tulkinnan varaa. Ja selkeä ohjeistus mikä taho vastaa lisäkysymyksiin tietosuojasta.
Käytännönläheisiä esimerkkejä, mahdollisuus osallistua itselle sopivaan aikaan.
Konkreettisempia case- harjoituksia yksikön haastavissa tilanteissa, eikä yleispäteviä case tapauksia

Q21: What type of training would you best fit to learn concrete data protection situations?

Organisaation yhteinen, jossa huomioidaan sosiaali- ja terveysalan kaikki erilaiset toimintaympäristöt.
Real life scenarios tailored to my work setting and on specific context.
Netti. Testien ja tehtävien muodossa. Lukeminen on tylsää
Minulle sopisi parhaiten etäopetus tai verkko-opetus.
Kirjallinen materiaali
I am not sure
Verkkokoulutus omaan tahtiin.
Havainnollistava verkkokoulutus
Verkkokurssit ovat ihan hyviä, kunhan ne on pedagogisesti hyvin toteutettuja
Verkossa. Selkeät esimerkit.
Verkkokoulutus, johon saisi työaikaa.

Luennot

Keskusteleva

Having a hands on practical trainings with different cases, but not just most common and simple once, but more complicated that makes you think further and be proactive when dealing with cases at work after all.

Netti.

Etä varmaankin käytännöllisin, mutta ihan läsnä olo kurssina olisi paras

I don’t know what is available to choose from

Verkkokoulutus on useimmiten hyvä ja toimiva, mutta toki jostain tietystä aiheesta voisi järjestää ihan livekoulutuksenkin.

Opettaja/luennoitsija johtoinen koulutus.

Etä, virtuaaliset alustat

Case harjoitukset

Lähiopetus

Elearning but practical about data

Presentations with questions about data protection that I need to answer to pass to the next phase of the course.

Monimuoto.

Sosiaalialan tietosuojaan erikoistuneen juristin pitämä koulutus, jossa olisi käytännön esimerkkejä tietosuojaan liittyvistä tapauksista ja oikeuden ennakkoratkaisuja aiheeseen liittyen.

AMK riitti itselle

Etäkoulutus, hyvä kouluttaja, luennoitsija

Työpaja yhdessä työkavereiden kanssa

Verkkokoulutus

Live-koulutus

Verkkokurssit

Keskusteleva ja koko tiimille järjestetty

Verkkokurssit, luennot

Juuri omaan yksikköön kustomoitu workshop tai nauhoitettu workshop (kunhan se vastaa nimenomaan oman työyksikön tarpeita ja helposti ymmärrettävä sekä nopea käytännönläheinen ilman kapulakieltä)

On the job training

Käytännönläheiset koulutukset

Verkko-opinnot

Varmaan verkossa toki mielummin, koska asia on vähän kuivaa. Mutta ehkä jotkut hyvin visuaaliset ja esin pelin muodossa tapahatuvat voisivat jäädä paremmin mieleen.

Verkkokurssit

The most effective training format for me would be hands-on and situation-oriented — for example, workshops or simulations where we analyze and solve real data protection cases. This approach helps translate theory into practice and prepares me to handle concrete data protection challenges confidently.

Café-tyyppinen. Välillä haluaisin keskustella tietosuojaasioista suoraan ihmisten kanssa ettei aina olisi vain verkkokursseja-/luentoja.

nettikoulutus

Verkkokurssimaista, lyhyttä ja ytimekästä

Asiantuntija vierailu yksikössä.

Avoin keskustelu aiheesta asiantuntija vetoisesti.

Ennenvanhaan joku piti luennon, siinä oppii parhaiten ja voi kysyä jos jotakin nousee mielenpäälle

Verkkoympäristö

Surveys with facts that would “shock” someone in what is or what is not data protection

Case studies

Verkkokoulutus perustietoihin, jonka voi tehdä kun sopiva hetki ja lisäksi ihan kouluttajan johdolla oleva, jossa voi esittää kysymyksiä

Practical training

Koulutus jossa ollaan paikalla fyysisesti

Dangers

Etäkoulutus.

Netti tai koulutus työpaikalla

Itsenäinen opiskelu, tiimissä asioista keskusteleminen ja ryhmätyöt.

Verkkokurssi on käytännöllinen, mutta ei aina paras. Parhaiten opin itse, kun voi keskustella

I don't know

Case ratkaisut

Verkko

Lähikoulutus

Lyhyet case-videot

Itseopiskelu esim. Moodle alustalla

Verkko-opetus

Teams

Ryhmässä verkossa/paikan päällä

Verkkokoulutus

Ryhmämuotoinen lähikoukutus tai caseihin liittyvä etäkoulutus

Esimerkiksi teams, jossa osallistujiakin osallistetaan. Ei toimi ison ja vieraan ryhmän kanssa.

Case tyyppiset harjoitteet

Kts.yllä

Simulaatio

Nettikurssi, joka vie mahd. vähän resursseja, esim ehtisi tekemään töiden ohessa

Verkkokoulutus

Verkkokoulutus

Verkkokoulutus

Verkkokurssit

Case esimerkein

Verkkokoulutus. Pieniä tehtäviä mukana .

face-to-face and online training

Paikalla ollessa esim ryhmässä tehtäviä tilanteita

I don't know

Livekoulutus

Etä- ja itsenäisesti tehtävä.

Videot, keskustelut, testit

Interaktiivinen, tentin sisältävä jotta tulisi oikeasti opeteltua asiat.

Lähiopetus työaikana työpaikalla

Live koulutus

Webinaari, seminaari.

Verkkokoulutus itselle paras, mutta paikan päällä oleva koulutuksesta jää enemmän muistiin, jos kouluttaja on hyvä.

Luento- ja harjoitus

Webinaari

Verkkokoulutus ja lisäksi lyhyt yksikkökohtainen live koulutus

Q23: What kind of information do you feel you need more of?

Työskentely-ympäristöön käytännössä sovellettavaa.

Pitkä työkokemus, niin on asiat hallussa.

Toivoisin saavani lisää tietoa muun muassa siitä, kenelle asiakkaan/potilaan henkilötietoja voidaan luovuttaa. Minkälainen lupa asianomaiselta asiakkaalta/potilaalta tarvitaan henkilötietojen luovuttamiseen?

En mitään

Information regarding keeping data safe online, pseudonimation and anonymisation processes

Client privacy rights

Helposti löydettävää tietoa. Kaikkea ei tarvitse osata ulkoa, mutta välillä tiedon etsimiseen menee tuhottomastai aikaa. Myös joskus tieto on oman tulkinnan varassa, joten "kansantajuisesti" selitetty

Lasten

En kaipaa lisätietoa.

Kaikkia edellämainittuja

Varmasti ihan kaikenlaista

Reporting on data breach

All kinds

Ajattelen osaavani melko usein, mutta tiedon ylläpitämiseksi, voisi tietosuojaan liittyä jonkinlainen kertaus säännöllisin väliajoin.

Olisi hyvä kerrata lait, asetukset määräyksen juurikin käytännön toiminnan tasolla

Miten tietosuojaa noudatetaan opiskeluhuollon kontekstissa

Pracical training

How to report problems

När en incident ska rapporteras

Käytäntöä.

Tietoa sosiaalihuollon Kanta-siirtymästä.

En tarvitse. Ongelma on siinä ettei kukaan noudata gbdr asetuksia ja sosionomin töitä tekevät lähihoitajan eivät ole tietoisia.

Miten tulee toimia, jos tietosuojakäytänteet eivät vastaa GDPR ja hallinto on sitä.mieltä, että suoja on riittävä?

Syvemmän tason ymmärrystä. Sellaista, joka tukee tietosuojavastaavan työtä.

Clarification in cases where a 3rd party is involved (for example parents or children who handle the business of the patient)

Kollegojen puolesta sanoisin, että väärin tehdyt postitukset, toisen asiakkaat kirjaukset toisen asiakkaan tiedoissa jne on yleisiä. Ja esim ei-huoltajalle luovutetut tiedot.

Ei näitä ymmärretä ja virheitä vähätellään. Asioita peitellään, eikä ilmoiteta eteenpäin. Tai esim neuvottelussa puhutaan asioita, jotka eivät kuulu kaikille läsnäolojoille.

Välillä kauhistuttaa! Silti kaikki sanoo, että kyllä me osataan ja itsestään selviä asioita. Ei osallistuta koulutuksiin. Näiden pitäisi olla pakollisia läsnäolokoulutuksia. Ei videoita ja monivalintatehtäviä. Koulutuksissa esimerkkien kautta työskentely olisi tärkeää.

Oman yksikkööni kustomoidut ohjeet, eli case/tilaneteita top 5 mitä tapahtuu/voi tapahtua/ei pidä tapahtua ja selkeä polku tee ilmoitus tästä

Tarkempaa ja syvempää tietoa, asia on kuitenkin tärkeä

En tällä hetkellä koe tarvitsevani lisätietoa.

Ethical and legislation surround it

Tietoturvaloukkausten selvittämiseen.

Mitä ne potilaan oikeudet ovat

Pratical information of day-to-day situations where data protection might be at risk

En tällä hetkellä koe tarvitsevani. Ohjeet hyvin saatavilla

Tarkennusta miten tietoja käsitellää ja säilytetään. Miten parantaa osaston käytäntöjä turvallisemmaksi

Joitakin käytännön asioita.

Easy to digest information about data protection

Taloudellisen edunvalvonnan asioissa

Organisaatiossani tietopyynnöt on keskitetty. Hieman epäselvää on, kuka arvioi/päättää luovutetaanko pyynnön mukaisesti.

En osaa spesifioida mitään, mutta välillä tulee hyvin harvinaisia poikkeustilanteissa, joihin olisi hyvä olla varautunut.

Tiedon jakaminen

Käytännön esimerkkejä

Asiakkaalle annettavaa tietoa selkokielellä

Mitä tehdä silloin, kun tietosuojaohjeita on jostain syystä mahdoton noudattaa.

Tiedon päivittämistä ja uusista huomioista tietosuojaan liittyen

En tarvitse, pitkään ollut alalla

GDPR

En juuri mitään. Olen toimipaikkani tietosuojavastaava

En mitään

Vaikea määritellä, koska oma tunne on, ettei kokonaisuus ole riittävästi hallussa

Updates of new cybersecurity related threats

I don't know

Nykyisen virkani vuoksi tunnen asian hyvin. Organisaation koulutus ei ole tätä osaamista taannut.

Tarkennuksia käytänteisiin potilaan pyytäessä omia tietojaan

Ei tule mieleen mitään mikä voisi itseä enemmän auttaa

Q25: What kind of practical changes or needs have you identified in your work unit in relation to data protection?

*Toimistossa näyttöpäätteiden näytöt ovat suunnattuna sisäänkäynnin suuntaan. *Tietoturvajäteastia on vain yhdessä neljästä rakennuksessa toimivasta yksiköstä. Käyttö jää vähäiselle. *Henkilökunnan tietoturvatieto vähäistä. Whatsup-sovellusta käytetään talon asioiden tiedottamiseen ryhmässä. Työvuorolistalle on ulkopuolisilla pääsy. Työskentely-yksikössäni on tallentava kameravalvonta sisällä yleisissä tiloissa, tästä ei informoida asiakkaita eikä työntekijöitä.
Training on data protection should be continuous. One time-off trainings are not helping at all. Team members avoid to pay attention at all at data protection issues and they use in irresponsible manner test data.
Esim asiakastietoja tulostetaan turhaan. Teamsissa viestitään asiakkaista ym
En mitään. Meillä tietosuoja on erittäin tärkeä asia ja paukuteltu kaikille päähän uudestaan ja uudestaan.
Updates on regulations
Erilaisten nimilistojen keräykseen liittyvät asiat. Kun tarvitsemme paljon erilaisia listoja, missä niitä oikeasti voimme kätevästi säilyttää turvallisesti.
Ilmoittautumistietojen säilytysaika ja niiden käyttö.
En ole havainnut muutostarpeita.
Kaikkia ei tunne
Varmaan se liittyy ihan arkisiin asioihin, kuten missä keskustellaan asiakkaiden asioista (esim. ruokala, puhelut tms.) ja näiden iskostaminen "selkäytimeen".
Tietosuoja ei aina toteudu. Henkilöt, jotka eivät työskentele asiakkaiden kanssa, ovat kuitenkin läsnä kun asiakkaiden asioita käsitellään. Asiakastietoja sisältäviä papereita on työpöydillä. Jaetuissa työtiloissa muut kuulevat esim puhelinkeskusteluja. Työtilat eivät ole äänieristettyjä.
Lisää tietoa
None
Paperisia tietoja vähemmän.
Keskustelua on työyksikössä käyty tietojärjestelmien riittävästä tietosuojasta henkilötietojen yhteydessä. Reaktiivisen valvonnan osalta tietosuojan huomioiminen.
Sen ettei GBDR.ää noudateta
No sitä pitäisi varmaan noudattaa

Työntekijöille on pitänyt huomattaa, että asiakaasta voi laittaa nimiä seinälle tai papereita säilyttää tulosteina

Toiminnan muutoksen tarpeita. Tietosuojaa ei pidetä tärkeänä.

Valtaosa kolleegoista on vieraskielisiä, eikä suorastaan ymmärrä mistä on kyse vaikka tietosuojakiulutusten jälkeen pidetty yhteinen treenitunti, niin eivät sielläkään ymmärrä

Sähköpostiosoitteiden ongelmat isossa organisaatiossa missä voi olla saman nimisiä työntekijöitä.

Salasanat voisivat olla varmempia

We've noticed that data protection could be strengthened through clearer procedures for classifying and storing data, as well as regular staff reminders about secure data handling. Additionally, implementing standardized templates for consent and data-sharing agreements would help ensure compliance and reduce uncertainty among staff

Papereiden säilyttäminen ja väliaikainen arkistointi.

Paperin hävitys muuttunut turvallisemmaksi. Tietokoneen käyttäjän vaihto olisi sastava helpommaksi, ohjelmien avaaminen nopeammaksi

Tietosuojavastaavan rooli työyksikössä ei ole ollut kovin näkyvä. Tietosuojavastaavan saaman lisäkoulutuksen kautta nostettu keskusteluun erilaisia huomioita aiheesta.

Useimmiten tietosuojaan liittyvät kysymykset nousseet esiin auditoinnissa.

Yrityksen ohjeistukset ovat ristiriitaisia keskenään

Jonkinlainen tietosuojan huoneentaulu olisi hyvö saada jokaiseen toimipisteeseen.

Difficulty on protecting patient data while discussing clinical cases (metioning names, giving details on the presence of others, sometimes on informal places, e.g. cafeteria, Open treatment áreas)

Mitä muiden asiakkaiden asioista saa puhua muille asiakkaille. Jotkut eivät ymmmärrä ettei asukkaiden asioita puhuta muiden kuullen

Meille on tullut uusia työntekijöitä ja uusi tietosuojavastaava (työskennellyt ennen eri organisaatiossa aivan eri tehtävissä). Tiedonkulku asioihin liittyen henkilöstön vaihtuessa varmistettava.

Ns paperitietojen säilyttäminen asiakkaille/omaisille/siivoushenkilöstölle muille. Ei oikein ole myöskään tiloja esim puheluiden käymiseen, jossa ei olisi muita ihmisiä. "Käytäväraporteissa" rikotaan varmaan kaikkia salassapidon säädöksiä...

Teams keskusteluissa ei välitetä enää mitään asiakkaiden asioita.

Hyvinvointialueiden vaatimukset

Tietosuoja ei toteudu avokonttorissa, jossa puhutaan asiakaspuheluita

Paperien hävittäminen, säilyttäminen, asiakkaille ei selitetä asioita maallikolle soveltuvalla tavalla

Ohjeet ovat tiukentuneet todella paljon, mutta käytännön toteutusta ei ole tarkasteltu.

Ei saisi olla mitään asiakastietoja papereilla ym.

Apotti - asiakkaiden viestit tulevat työkoriin KOKO työryhmälle. Kerron tästä aina asiakkaalle, ja sanon, ettei työkoriviestiä Maisasta kannata laittaa. Mitä, jos minulla on asiakkaana työkaverini kaveri/tuttava/läheinen/perheenjäsen?
Yhteiskäyttötiloissa tietosuojan toteutuminen pitää huomioida erikseen
Uusi atk-järjestelmä voi olla vähän haasteellinen
Eri asiakastietojärjestelmien päivitysaikataulut ja niiden vastuut ovat epäselvät eri käyttöympäristöissä
Organisaation ohjeet ovat vaikeasti löydettävissä ja siksi on vaikea sanoa uskottavasti, että pystyy itse toimimaan ja ohjaamaan asiakkaita niiden mukaisesti.
Implementations of GDPR and other regulations into everyday work
I have not
Sote uudistus loi suuria riskejä, joita toki pyritty taklaamaan.
En ole havainnut viime vuosina suurempia muutoksia. Osa kollegoista kertoo melko avoimestikin potilastietoja esim. potilaan kanssa samassa taloudessa asuvalle vaikka ei ole aina tarkistanut potilaan kantaa tietojen luovutukseen. Osa taasen toimii oikein kuten edellytetään.
Tietosuoja jätettä tulee paljon, käytössä huoneissa avoimet laatikot jotka kolmas osapuoli tyhjentää.
Välillä työkaverit unohtavat rajat ja puhuvat liian avoimesti.

Q27: In general, briefly describe which data protection issues have been addressed in your work unit recently.

Asiakkaiden sosiaali- ja terveystietoja.
Kanta-palveluun siirtymiseen liittyviä
Että varsinkaan tuttujen tietoja ei katsota.
Papereita
Erilaisten nimilistojen säilytykseen ja jakamiseen liittyviä
Asiakkaiden henkilöllisyystietoja ei saa kertoa, näyttää, kuvata kenellekkään/ mihinkään.
Vapaaehtoistyöntekijöiden tiedot. Arvontalappujen tietojen näkyminen. Ja vaikka mitä.
Kaikki ovat nyt syksyllä suorittaneet tietosuojatentin.
Meillä tarvitsee käydä kerran tietosuoja ABC, siinä se.
Running surveys for the correspondents on the epidemiological data.
Potiasasiakirjamerkintöjen oikaisuvaatimukset
Viimeksi tapahtuman järjestämisen yhteydessä asia nousi esiin.
Lähiaikoina ei mitään
Fraud emails
Diskuterande av patientinfo med samarbetspartner

Pakollinen Beeware- kurssi.

Tietopyyntöjen yhteydessä luovutettavat tiedot läpikäyty salassapidettävien tietojen osalta.

Ei käsitellä, potkut tuli sille joka otti puheeksi.

'Olisi hyvä tietää" tai "tukisi asiakasta" tyyppisiä ajattelumalleja, joissa työntekijä ajattelee että jonkun toisen olisi hyvä tietää jotain asiakkaasta tai että asiakasta tukisi, jos hänen nimensä lukee nähtävillä

Henkilötietoja on löytynyt verkkolevyiltä ja ollut näkyvillä sellaisille henkilöille, joilla ei ole oikeutta kyseisiin tietoihin organisaation sisällä.

Tietosuojajätteen käsittelyä, tietosuojaa eri yksiköiden työskennellessä samoissa tiloissa.

Skannaukseen lähtevistä papereista puuttuu asiakkaan id-numero

Handing over data to parents for children and the assessment of children's ability to decide about their data independently

En muista, että mitään

Viime aikoina ei mitenkään. Pakolliset kurssit itsenäisesti suoritettava, eipä muuta

Tietojen jakamiseen liittyviä asioita

Missä ja minkälaista tietoa voi säilyttää.

Recently, our work unit has focused on strengthening data protection practices by reviewing data storage procedures, updating consent forms, and raising awareness about secure data handling and confidentiality.

Papereiden säilyttämistä.

Ei kuulu työnkuvaan, tietosuoja-asioita hoidetaan muiden toimesta

Poikkeusilmoitusten käsittely koskien tietosuojaa mm. salassa pidettävän kirjallisen materiaalin käsittely ja säilöntä.

Esihenkilötyöryhmässä pohdittu yleisesti työntekijöiden osaamista ja ymmärrystä koskien tietosuojaa.

Kuukausikoosteiden lähettämistä sähköisesti hyvinvointialueille

This issue was never adressed, as many do not identify it as a problem, it is part of the organization's culture.

Tietojen luovuttamiseen ja säilyttämiseen liittyviä. Etätyöhön liittyviä.

Henkilötietoja sisältäviä asiakirjoja on siirretty eri paikkaan (tietoturvallisempaan). Eri toimialat ja yksiköt on vastuutettu itse huolehtimaan tietyistä asioista, niihin saa tukea organisaation tietosuojavaltuutetulta.

Henkilötietojen käsittelyä ja tiedonsiirtoa käsitellään usein tiimin keskusteluissa.

Menty vääriin potilaspapereihin asiakkaan luetellessa hetu väärin, tai ilmoittautunut eri perheenjäsenen kortilla kuin sen, jonja asiaa hoitaa, kotihoitaja ilmoittautuu omalla tunnuksellaan vaikka hoitaa asiakkaan asiaa

On pidetty erillinen tietosuojakoulutus tiedon tallentamiseen.

Esim missä kaikkialla on tunnistetiedot henkilöistä.

Moniammatillisten tiimien kokoonpano

Viime aikoina on käsitelty sitä, miten ja millä asiakkaiden ja asiakasperheiden kanssa viestintään, eli missä viestit lähetetään ja mitä tietoja ne sisältää.

Ei ole käsitelty mitään

Meidän työyksikköön tulee käsiteltäväksi muissa yksiköissä esiin tulleet tietosuojapuutteet ja ohjaamme yksiköitä niiden osalta jatkuvasti.

Lakisääteisten taustatietojen toimittamista hoitajille. Asiakkaan henkilötietoja ei saisi olla lomakkeella, mutta lain mukaan hoitajalla on niihin oikeus. Mietimme nyt miten ja missä vaiheessa mitäkin tietoja voi toimittaa. Myös hoitajien tietoturvan varmistamista

Excell listojen käyttämistä suojatussa ympäristössä. Kaikki pitäisi olla apotista

Esim.juuri Apotin työkoriviesteistä on keskusteltu

Teamsin käyttö potilaskontakteissa

Salassapitovelvollisuutta koskien työtekijöiden perheiden asioita.

Tuli huomautus että yli 100 työntekijää on käynyt omissa tiedoissaan hva:lla. Tämä on kiellettyä-jostakin syystä.

Salasanan lähettäminen yhteiskäyttöpuhelimeen. Asiakastietojärjestelmistä puutteellinen uloskirjautuminen, Asiakastietojärjestelmän mobiilisovelluksen tietoturvan päivityspuutteet

phishing scams

Can't remember.

Tietoturvasta puhutaan virassani jatkuvasti. Tietoturvasuunnitelmaa tarkastellaan.

Saako osastolle soittavalle henkilölle kertoa onko joku tietty henkilö osastolla potilaana? Vastauksia kerrotaan melko vapaasti vaikka itse en kerro kysymättä lupaa heti potilaan saapuessa (Lupa potilaalta kenelle saa tietoja luovuttaa).

Yhteiseen työkoriin tulevien viestien sisältö. Mitä on tarpeen jakaa koko työyhteisölle, mitkä olisi hyvä jakaa vain hoitavan lääkärin/hoitajan kesken.

Isossa konsernissa ei ole tähän mahdollista.

Annex D Thematic Coding of Open-Ended Responses

The open-ended responses were analysed using inductive thematic coding. All answers were read through several times to identify recurring patterns, concepts and expressions. Based on this process, responses were grouped into thematic categories that represent the most common ideas expressed by participants. Each theme was assigned a binary code (0 = not mentioned, 1 = mentioned), allowing the qualitative material to be quantified and used alongside the quantitative analysis.

The themes and their corresponding codes are presented below for each open-ended question:

Q20 – Preferred type and format of training
Practical examples (T20_1), Clearer materials (T20_2), In-person training (T20_3), Online training (T20_4), Unit-specific training (T20_5), Regular training (T20_6)

Q21 – Best format for learning practical data protection situations
Simulations (T21_1), Workshops (T21_2), Case examples (T21_3), Online modules (T21_4), Peer learning (T21_5)

Q23 – Information needs
GDPR principles (T23_1), Practical procedures (T23_2), Data breach reporting (T23_3), Rights of clients/patients (T23_4), Special categories of personal data (T23_5)

Q25 – Practical changes or needs in the work unit
Improved instructions (T25_1), Better systems (T25_2), More training (T25_3), Improved processes (T25_4), Communication needs (T25_5)

Q27 – Recent data protection topics addressed in the work unit
Data breaches (T27_1), Guidelines (T27_2), System changes (T27_3), Rights of clients/patients (T27_4), Risk management (T27_5)

The thematic coding process resulted in several recurring themes across the open-ended questions. These themes represent the most common types of responses, such as requests for more practical examples, clearer instructions, improved systems, or more frequent training. Each theme captures a specific pattern in the data and was assigned a binary code (0 = not mentioned, 1 = mentioned) to enable quantitative analysis of qualitative content.