
Metasoul: Exploring Digital Legacies and Post-Mortem Data Rights

Conceptualising post-mortem data management through legal
frameworks, user experience, and service providers

Master Thesis
Group 1002

Aalborg University
Electronics and IT



AALBORG UNIVERSITY
STUDENT REPORT

Electronics and IT
Aalborg University
<https://www.aau.dk>

Title:

Metasoul: Exploring Digital Legacies and Post-Mortem Data Rights

Theme:

Master Thesis

Project Period:

Spring Semester 2025

Project Group:

Group 1002

Participant(s):

Abedallah Ajjawi
Rasmus Beyer Andersen
Simon Shahrour

Supervisor(s):

Lene Tolstrup Sørensen
Amar Djebbara

Main report page numbers: 105

Total page numbers with appendices: 137

Date of Completion:

June 4, 2025

Abstract:

As digital lives increasingly outlast their owners, managing data after death poses a growing challenge for individuals and families. This thesis explores post-mortem data practices and introduces the Unified Post-Mortem Access Protocol (UPAP), a protocol for standardising service provider practices. The thesis applies a threefold exploration of legal frameworks, user experiences, and service provider practices to examine how digital assets are managed after death. Methodologically, it combines legal exploration with focus on Denmark, and Scandinavian countries for comparison, with the analysis of service providers, a user survey of 140 individuals, and interviews to capture user perspectives. The main issue is the absence of clear laws and standards for post-mortem data handling, creating uncertainty around privacy and access. Findings show legal variation, inconsistent service provider practices, low user awareness, and a complex process for next of kin handling legacies of the deceased. The thesis concludes that legal reform, user awareness, and a protocol like UPAP are potential steps toward better handling of digital identities after death. This thesis also aims to encourage future work in the unexplored field of post-mortem digital rights.

Keywords: digital legacy management, post-mortem rights, unified post-mortem access protocol, metasoul

The content of this report is freely available, but publication (with reference) may only be pursued due to agreement with the author.

Preface

This thesis was completed by Group 1002 during the Spring semester of 2025 as part of the Cyber Security Master's program at Aalborg University, under the theme *Post-mortem data rights*. The thesis was supervised by Lene Tolstrup Sørensen and Amar Djebbara.

Acknowledgements

We extend our deepest gratitude to our supervisors, Lene Tolstrup Sørensen and Amar Djebbara, for their guidance and support throughout this thesis. Their expertise and feedback have been significant in shaping our work.

We also thank Astrid Waagstein, PhD, for her insights on post-mortem data rights, Bilal Bahij and Janni Brodersen from the IT department at Syddansk Universitet for their assistance in understanding organisational processes, a Professor in Privacy Engineering for their helpful advice. We also extend our thanks to Sakariye Mahamed and Johan Niordson for their time and valuable insights.

Finally, we acknowledge the authors and researchers whose work laid the foundation for our thesis, and we are deeply grateful to our families and friends for their continued support.

Disclosure of generative AI utilisation

Generative AI tools, Perplexity and ChatGPT 4o, were used to refine language, suggest synonyms, and assist in formulating survey and interview questions. In the data analysis phase, AI supported the development of scripts, however, all methodological design and core coding were carried out by the group. The use of AI was supplementary and did not replace original academic work.

Abedallah Ajjawi

Abedallah Ajjawi

<aajjaw23@student.aau.dk>

Rasmus Beyer Andersen

Rasmus Beyer Andersen

<rban23@student.aau.dk>

Aalborg University, June 4, 2025

Simon Shahrour

Simon Shahrour

<sshahr23@student.aau.dk>

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 3 |
| 1.1 | Background and motivation | 3 |
| 1.2 | Goal of the thesis | 4 |
| 1.2.1 | Scope and delimitations | 5 |
| 1.3 | Thesis Structure | 5 |
| 2 | Background | 7 |
| 3 | State of the Art | 10 |
| 3.1 | Literature review | 10 |
| 3.2 | Existing commercial solutions | 14 |
| 4 | Methodology | 16 |
| 4.1 | Legal Frameworks | 16 |
| 4.1.1 | Denmark & other Scandinavian countries | 17 |
| 4.1.2 | China's Personal Information Protection Law (PIPL) | 17 |
| 4.1.3 | European regulatory frameworks for digital governance | 17 |
| 4.2 | Service Providers | 18 |
| 4.2.1 | Service Provider Data Analysis | 19 |
| 4.3 | Data Collection | 20 |
| 4.3.1 | Quantitative Survey | 20 |
| 4.3.2 | Qualitative Interviews | 23 |
| 4.4 | Proposal of a proof of concept | 25 |
| 4.4.1 | Evaluating architectural approaches | 25 |
| 4.4.2 | Workshop process and protocol design | 25 |
| 5 | Exploration of Legal Frameworks | 27 |
| 5.1 | Danish Data Protection Act | 28 |
| 5.2 | GDPR and PIPL | 28 |
| 5.2.1 | GDPR | 28 |
| 5.2.2 | PIPL | 28 |
| 5.2.3 | Comparative evaluation between GDPR and PIPL | 29 |
| 5.3 | Scandinavian context | 29 |

| | | |
|-----------|--|-----------|
| 5.3.1 | Norway | 29 |
| 5.3.2 | Sweden | 30 |
| 5.4 | European initiatives | 31 |
| 5.4.1 | The role of eIDAS 2.0 in digital legacy management | 31 |
| 5.4.2 | Review of European Law Institute (ELI) on digital inheritance | 31 |
| 5.4.3 | Fairness and responsibility in the EU digital space | 32 |
| 6 | Analysis of Service Providers | 34 |
| 6.1 | List of Service Provider policy resources | 37 |
| 6.2 | Passive deactivation procedures | 38 |
| 6.3 | Reactive user and post-mortem procedures | 42 |
| 6.3.1 | Legacy contact, pre-assigned heir or emergency access | 42 |
| 6.3.2 | Next of kin or legal request | 44 |
| 6.3.3 | No support process | 47 |
| 6.4 | Service provider risk assessment | 48 |
| 6.5 | Overview of findings and insights | 51 |
| 7 | Analysis of Survey and Interviews | 52 |
| 7.1 | Quantitative survey results | 52 |
| 7.2 | Qualitative interview results | 63 |
| 8 | Summary of findings | 67 |
| 9 | Proposed solution | 69 |
| 9.1 | Problem definition and scope | 69 |
| 9.1.1 | Scope of service providers | 70 |
| 9.2 | Requirements specifications | 70 |
| 9.3 | Core Principles and Compliance | 72 |
| 9.4 | Technical Architecture | 73 |
| 9.5 | Implementation considerations for service providers | 84 |
| 9.6 | Proposal for validation and testing metrics | 85 |
| 10 | Discussion | 87 |
| 10.1 | Recurring themes and proposed solution | 87 |
| 10.1.1 | User awareness, behaviour, and barriers in digital legacy planning | 87 |
| 10.1.2 | Bridging the gap between user needs and post-mortem data solutions | 88 |
| 10.1.3 | Legal Gaps and the need for harmonised regulation | 89 |
| 10.1.4 | Alternative solutions and design justification | 90 |
| 10.2 | Limitations | 91 |
| 10.2.1 | Legal framework analysis | 91 |
| 10.2.2 | Service providers analysis | 91 |
| 10.2.3 | Interview handling | 91 |

| | |
|---|------------|
| 10.2.4 Proof of concept | 91 |
| 10.3 Future work | 92 |
| 10.3.1 Verification of death certificates | 92 |
| 10.3.2 Implementing and testing a MVP of UPAP | 92 |
| 10.3.3 Threat modelling the post-mortem landscape | 93 |
| 10.4 Ethical considerations | 93 |
| 11 Conclusion | 95 |
| 11.1 Concluding summary | 96 |
| 11.1.1 Assessing legal readiness for post-mortem management | 96 |
| 11.1.2 Lack of standardisation for service providers | 96 |
| 11.1.3 Findings from survey and interview analysis | 97 |
| 11.2 Proposed solution | 97 |
| 11.3 Impact and Contributions | 98 |
| 11.4 Future research directions | 98 |
| 11.4.1 Commercial motives | 98 |
| 11.4.2 Psychological aspect | 98 |
| 11.4.3 Cultural considerations | 99 |
| Bibliography | 100 |
| Appendices | 106 |
| Appendix A: Qualitative Interview Questions | 106 |
| Appendix B: Unified Post-Mortem Protocol exploration Miro board | 110 |
| Appendix C: Quantitative survey data | 127 |

Glossary

Danish Data Protection Act The national law implementing the GDPR in Denmark, officially titled *Databeskyttelsesloven*, which supplements and specifies how EU data protection rules apply in the Danish context.

Dedicated DLMS Dedicated Digital Legacy Management System: A standalone system specifically designed to manage digital legacy planning, storage, and access.

DMA Digital Markets Act: A regulation by the European Union designed to ensure fair and open digital markets by targeting large online platforms acting as *gatekeepers*.

DSA Digital Services Act: A regulation by the European Union aimed at creating a safer digital space by establishing a single set of rules for online platforms and intermediaries across the EU.

EEA European Economic Area: An agreement that extends the European Union's internal market to non-EU countries such as Norway, Iceland, and Liechtenstein.

EIDAS 2.0 An updated EU regulation aimed at enhancing digital identity frameworks across member states, introducing the concept of a European Digital Identity Wallet for secure and interoperable online authentication.

ELI European Law Institute: An independent organisation that evaluates and provides guidance on legal developments within Europe.

EU European Union: A political and economic union of 27 European countries that are located primarily in Europe and operate through a system of supranational institutions and intergovernmental decisions.

GDPR General Data Protection Regulation: The European Union's legal framework designed to protect individuals' personal data and privacy.

HCI Human-Computer Interaction: The study and practice of designing user interfaces and interactions between people and computer systems.

Integrated DLMS Integrated Digital Legacy Management System: A digital legacy management solution embedded within existing platforms or services, such as social media or cloud providers.

Memorialisation The process by which a deceased person's digital account is preserved in a way that reflects their passing, often with restricted access or special status.

Metasoul A term introduced in this thesis to describe the dynamic, post-mortem digital presence of an individual, encompassing digital assets, identities, memory, emotion, and ongoing interactions beyond death.

MVP Minimum viable product: The simplest version of a product that can be released to demonstrate its core functionality.

NOK Next of kin: The closest living relatives of a deceased person, often responsible for managing their estate and affairs.

PIPL Personal Information Protection Law: China's legal framework for regulating the collection, use, and storage of personal data.

POC Proof of concept: An initial implementation or prototype designed to demonstrate the feasibility of a proposed solution.

UPAP Unified Post-Mortem Access Protocol: A proposed standard protocol developed in this thesis to guide service providers in managing digital legacy and post-mortem data access.

Chapter 1

Introduction

1.1 Background and motivation

In today's society, individuals interact with a wide range of digital accounts, including but not limited to, social media profiles, email services, cloud storage, banking platforms, and subscription-based applications. As digitisation accelerates, people increasingly generate, store, and share data across these services, thereby expanding their digital footprint. This growing accumulation of digital personal information makes such accounts appealing targets for cyber criminals, who may exploit them for financial gain, identity theft, or other malicious purposes.

Fortunately, legal frameworks such as the General Data Protection Regulation (GDPR) in Europe aim to protect the rights of users and hold service providers accountable. Many providers have also implemented security measures like login notifications, password reset alerts, and two-factor authentication (2FA) to improve protection. Despite this, the cyber security landscape remains a constant *cat-and-mouse* game, where adversaries attempt to gain an edge over defenders.

But what happens when the person behind the digital accounts is no longer alive? After death, who becomes responsible for protecting their online data? Does this responsibility fall to the service provider, or is it left to surviving relatives? Are there clear policies for managing access to different provider after the death of a user? As digitally native generations grow older, these questions are becoming increasingly relevant for individuals, families, and service providers.

This thesis was motivated by a real-world incident that drew attention to the challenges of managing digital accounts after death. Although some service providers offer basic features such as memorialisation or account deletion, there is still a lack of clarity in how these policies are communicated and implemented. Questions around access, data protection,

and responsibility often remain unresolved when a user passes away.

On a December evening in 2023, one of the authors received a Snapchat notification from a friend who had passed away in a car accident four years earlier. The account had been compromised, and private content was being shared publicly, including messages sent to friends and family. It was later discovered that the phone of the deceased person had been stolen during the accident, which granted access to several accounts. Despite multiple reports, the service provider responded with a standard message, stating that nothing violated their terms of service.

This experience drew attention to how digital identities may remain active and potentially vulnerable after death, and it served as the initial inspiration for exploring how digital legacies are currently managed.

This experience sparked the interest in the topic, and initial research confirmed that the mismanagement of digital identities of deceased individuals is a challenge for many. For instance, a survey of 400 participants[37] found that most had never considered what should happen to their data after death, despite concerns about privacy and identity theft. Similarly, another study[38] about exploring conflict in managing post-mortem data, showed that even security conscious users recognised the need for digital legacy planning. However, they often postponed taking action, showing how this issue extends well beyond a single personal experience.

1.2 Goal of the thesis

The goal of this thesis is to conduct an analysis of the current landscape of post-mortem data management and use that analysis to design and develop a proof of concept in the form of a standard protocol, referred to as the Unified Post-Mortem Access Protocol (UPAP). The analysis is based on both quantitative and qualitative survey data to assess current user experiences and challenges, along with a review of a range of service providers and relevant legal frameworks, primarily in Denmark and across selected jurisdictions.

The design and development decision in regards to UPAP is guided by addressing the questions of how the current landscape of post-mortem data management is structured, and how existing processes function for service providers, the user and next of kin. In conclusion the research throughout this thesis and development of UPAP provides the basis for answering the following problem statement:

How can digital legacy management be improved through the development of a conceptual solution that ensures secure, clear, and user-friendly handling of post-mortem data, in alignment with existing legal frameworks and the practices of digital service providers?

1.2.1 Scope and delimitations

This thesis primarily focuses on personal data belonging to individual users. While there are references to organisational or company data, as in the context of universities or specific cases from other countries, these aspects are not the main focus of the thesis.

The legal frameworks primarily focuses on Denmark, and includes other relevant laws. While not offering legal interpretations, the exploration highlights gaps and uncertainties in current regulation. Selected international perspectives, fellow Scandinavian countries and China, are included for comparison, but the focus remains on the Danish context. This focus is further defined and guided by the questions outlined in section 4.1.

Cultural differences in the handling of digital legacies are not explored in this thesis. While their relevance to decisions in relation to death is recognised, addressing such aspects would require interdisciplinary input from fields such as anthropology and sociology, extending beyond the scope of this thesis.

The proposed solution, described in chapter 9, is based on the findings of this research and is generalised for all service providers included in the thesis. The solution is not limited to Danish service providers, as service providers by nature often operate across national borders. No actual software or product development is done, as the primary aim is to explore the digital legacy management space.

This thesis aims to deliver a conceptual solution and a blueprint for a potential minimum viable product (MVP) implementation of post-mortem data management aimed at service providers. The purpose of the protocol is to propose core principles, technical architecture, and guidance on how to handle interactions with next of kin. Additionally, it addresses the resources required for implementation. While the protocol will not be tested in practice within the scope of this thesis, it is intended to provide a clear foundation for future development and deployment.

1.3 Thesis Structure

This thesis starts with an introduction in chapter 1 presenting the topic of digital legacy management, and outlines the problem statement as well as the goals and scope of the thesis.

Necessary background information and definitions of the core terms used throughout the thesis are provided in chapter 2. Additionally, all abbreviations and context specific terms is listed in the glossary above chapter 1.

In chapter 3 the current state of the art is presented, including a literature review in section 3.1 of other research on digital legacy management. In section 3.2 an overview of selected commercial solutions addressing this issue is presented.

Following this, chapter 4 describes the methodology throughout this thesis. This includes the exploration of legal frameworks in section 4.1 and analysis of service providers in section 4.2. It also covers quantitative and qualitative data collection methods, along with the analysis of the collected data, described in section 4.3. Finally, the chapter presents the methodology applied in the development of a proposed solution in section 4.4.

The research conducted is divided into three chapters with chapter 5 examining relevant legal frameworks, chapter 6 analysing service provider practices, and chapter 7 presenting results from surveys and interviews.

Together, these chapters provide the foundation for identifying requirements, gaps, and considerations. These insights are summarised in chapter 8.

In chapter 9 a proposed solution is introduced, outlining its overall architecture and the considerations that highlight its design. It draws on findings and insights from the preceding chapters, mapping these directly to the features and structure of the proposed approach.

The discussion in chapter 10 interprets the findings, considers their implications, acknowledges limitations, explores paths for future work, and addresses ethical considerations.

To conclude the thesis, chapter 11 summarises the main findings, highlights the impact and contributions of the thesis, and suggests directions for future research within the field of post-mortem data management.

Chapter 2

Background

This chapter provides foundational information used throughout the thesis. It introduces central concepts, describes relevant system types, and the roles of stakeholders involved.

Metasoul

The term metasoul is introduced in this thesis to move beyond a common definition of digital legacy. It is defined by Maciel et. al as *"the collection of digital assets, identities, and data traces left behind by an individual after death"*. [53] While legacy implies something to be inherited or deleted, the metasoul embraces the dynamic afterlife of digital identity. Including data that may remain active, be revisited, reshaped, or even revived. It includes not just digital assets, but also memory, emotion, and presence, reflecting how the digital footprint of a person can continue to influence and connect with others long after death.

Dedicated & Integrated Digital Legacy Management Systems

Managing the metasoul involves systems that support both pre- and post-mortem planning of the digital wishes of a person. In the literature, these are typically divided into two categories: Dedicated Digital Legacy Management System (Dedicated DLMS) and Integrated Digital Legacy Management System (Integrated DLMS) [53].

Dedicated DLMS are standalone platforms developed specifically for digital legacy management. These systems allow users to define instructions in advance, such as assigning next of kin (NOK), categorising content for saving or deletion, and sending scheduled messages after death. Their main strength lies in user autonomy and customisability. However, as they operate independently of service providers, they often face challenges related to integration, platform compatibility, and widespread adoption.

Integrated DLMS, on the other hand, are built into existing service providers such as social media or cloud services. Common examples include Facebook’s memorialisation settings[69] and Google’s Inactive Account Manager[77]. These systems offer features directly connected to the account of the user, but tend to be limited to the providers implementation. They provide only basic options for account management and operate under fixed service provider policies, with little room for user-defined preferences.

This distinction between dedicated and integrated systems highlights the gaps in both design of the systems and the policies they apply in regard to digital legacy management. Dedicated systems offer flexibility but rely on user engagement and trust in third-party providers. Integrated systems benefit from direct platform access but often lack transparency and fine-grained user control. Both represent different approaches to managing the metasoul.

Digital assets

Digital assets, as referred to in this thesis, includes the various online accounts and digital files that individuals collect throughout their lives. These assets are intangible and exist only in a digital form, in contrast to physical assets. Examples of digital assets include, but are not limited to:

- Social media profiles (e.g., Facebook, Instagram)
- Email accounts
- Digital photographs and videos
- Files stored in cloud storage services
- Cryptocurrencies and digital wallets
- Online gaming accounts
- Blogs and personal websites
- Messaging accounts

Stakeholders

While some service providers offer mechanisms for digital legacy management, it is also people and organisation who shape how the metasoul is managed. This section defines the stakeholders involved and the roles they play across planning, access, and post-mortem use.

Deceased individual

The deceased individual refers to the original owner of the digital accounts, data, and identities that make up the metasoul. Their digital footprint includes content created or stored across various service providers, such as emails, social media profiles, and media files. In the context of metasoul management, the deceased is considered in terms of any instructions or preferences set prior to death, including service provider settings or external documentation. Where no guidance exists, decisions regarding their digital presence are typically made by other stakeholders.

Service Provider

A service provider is any organisation that hosts, stores, or facilitates access to the digital content or identity of a user. This includes companies offering services such as cloud storage, email, social media, financial platforms, and subscription-based content. In metasoul management, service providers are relevant due to their terms, conditions, and tools for post-mortem data management. Their role is defined by the technical infrastructure they maintain, the user agreements they enforce, and any legacy planning features they offer.

Next of kin

In the context of this thesis, next of kin (NOK) are individuals who are designated, either formally or informally, to inherit or manage aspects of the digital presence of a deceased person. They may include family members, close friends, or legally appointed estate managers. In the context of metasoul management, NOK are often responsible for decisions related to the storing, deletion, or transfer of digital assets. Their role and extent of authority may be defined by legal ruling such as wills, service provider specific legacy contact settings, or local inheritance laws.

Chapter 3

State of the Art

This chapter presents a review of studies and perspectives that form the current State of the art in digital legacy research. It shows how researchers and system designers are approaching the challenges of digital legacy management, from emotional and ethical concerns to technical and design-focused questions.

3.1 Literature review

The papers reviewed addresses the topic from different angles. Grimm and Chiasson focus on everyday users and how they feel about using a centralised, possibly non-profit, service to manage their digital legacy.[37] Holt, Nicholson, and Smeddinck dive into the privacy side of digital legacy management, showing how even security-minded users often lack planning for what should happen to their accounts.[38] Maciel and Pereira take a broader view from the perspective of human-computer interaction, highlighting how death is still something digital platforms rarely plan for.[52] More recent work by Maciel et al.[53] and Akramov et al.[4] builds on this by looking at system requirements and legal frameworks for digital legacy management.

Survey on the Fate of Digital Footprints after Death

A technical report by Carsten Grimm and Sonia Chiasson, from Carleton University, titled *Survey on the Fate of Digital Footprints after Death*[37], explores how people would like their online presence to be handled after they pass away. The report is based on a crowd-sourced survey of 400 participants from the United States, the United Kingdom, India, and various Asian countries.

The findings show that participants of the survey had never really thought about what should happen to their digital legacy. However, when asked, people leaned toward either

permanently deleting their accounts or handing them over to a trusted person, such as a next of kin. There was also a clear preference for a non-profit organisation to run such a service, ideally one that would only take action upon receiving a verified death certificate.

Grimm and Chiasson also explored the reactions of the participants to the idea of a centralised service managing digital assets after death. Most respondents reacted positively, especially to features like deleting accounts or sending pre-written messages to loved ones. On the other hand, they were much less enthusiastic about services that rely on inactivity or frequent notifications asking if the user is still alive, used as a criteria for triggering account deletion.

Although the authors acknowledge some limitations and sensitivity of the topic, the study offers valuable information on how digital afterlife services might be designed to align with user expectations and ethical concerns.

From Personal Data to Digital Legacy: Exploring Conflicts in the Sharing, Security, and Privacy of Post-mortem Data

In the paper *From Personal Data to Digital Legacy: Exploring Conflicts in the Sharing, Security, and Privacy of Post-mortem Data*, the authors Jack Holt, James Nicholson, and Jan David Smeddinck[38] investigate how security conscious users think about their digital legacy after they pass away. The study is based on two workshops in which participants, mainly users of password managers, were asked to discuss and plan for a variety of digital assets in the event of their death.

One of the takeaways from the paper is what the authors call the post-mortem privacy paradox. The paradox describes that while participants recognised the importance of planning what should happen to their digital legacy when they die, most of them admitted that they had not done anything about it. There is this conflict between wanting to be secure and private while alive, but also wanting some of that data to be accessible or passed on after death. The research also showed that strong security habits like using password managers or multi-factor authentication can make it harder for loved ones to access important data after death. There is also a clear discomfort around the topic in general, with participants pointing out how thinking about death is not exactly something people look forward to. This kind of attitude seems to be one of the main barriers stopping people from actively making plans.

The authors propose that password managers and similar tools could be designed better to support digital legacy planning, like letting people decide which accounts should be deleted or shared, and with whom, after they die. They also recognise that for most users, especially those who are non-technical, this process would need to be simplified and more comfortable to think about.[38] Although the study only involved a small and fairly technical group of people, it still brings important points about the growing need

for digital legacy management. The paper highlights how privacy, technology, and human behaviour do not always align neatly, especially when death gets involved.

Post-mortem Digital Legacy: Possibilities in HCI (Human-Computer Interaction)

The paper *Post-mortem Digital Legacy: Possibilities in HCI (Human-Computer Interaction)* by Cristiano Maciel and Vinicius Pereira[52] explores how digital legacy management is becoming an increasingly important issue in the field of Human-Computer Interaction (HCI). The authors highlight how our growing reliance on digital systems for communication, work, and even memory keeping raises complicated questions regarding management of digital legacies.

The paper outlines how HCI researchers have begun to investigate the ways people interact with digital technologies at the end of life. The authors outline the rise of discussions around death in tech spaces, noting that although death is a universal experience, it is still a taboo topic in both society and system design. They point out that technologies like Facebook's memorialisation settings[69] or Google's Inactive Account Manager[77] are steps in the right direction, but there is still a gap in providing users real control over their digital legacies.

One interesting theme in the paper is the tension between storing and deletion. Some people want their digital legacy to live on, while others would rather have their legacies erased. This division creates a requirement for handling both cases when trying to build tools that should handle personal preferences. The authors suggest that designers need to consider aspects like cultural differences, legal systems, and even religious beliefs when designing for digital legacy management.[52]

The paper also addresses "*posthumous interaction*", as the way people continue to engage with digital profiles after the death of their owner. Whether it is visiting a profile or leaving comments on a memorial post, this form of post-mortem interaction is increasingly prevalent, and yet it is still not well supported by platforms. Overall, the paper acts as a reminder for the HCI researchers and developers. It is a reminder that digital legacies live beyond their owners, and that there is a need for tools and systems to address that transition.

Defining Digital Legacy Management Systems' Requirements

The paper "*Defining Digital Legacy Management Systems' Requirements*" by Maciel, Mendes, Pereira, and Yamauchi[53] tackles a growing need for systems that help individuals manage their digital legacy, data, content, and accounts that outlive them online. As digital platforms have become part of our personal and professional lives, the question of how to handle digital footprints after death is increasing attention, and this paper proposes a way

to start designing systems for post-mortem data management. The authors points out that existing platforms offer very limited tools for users to plan or control their digital legacy.

The paper argues for a more proactive approach, one where users can explicitly define what should happen to their data and digital presence through structured systems. Based on interviews, the paper identified a set of functional and non-functional requirements for digital legacy management systems[53]. These include features that lets users choose specific heirs for different assets, set access rules, or request deletions after their death. In terms of non-functional requirements, trust, privacy, and transparency were highlighted as elements that would increase willingness to digital legacy systems.

The papers focuses on a user-centered design approach. It identifies the systems capabilities, in relation to user needs, based on real-world scenarios and concerns. It discusses the emotional weight of digital legacy management, recognising that for systems to meet user needs in this context, it requires a cultural and personal perspective, which is often overlooked in technology design[53].

The Impact of Digitalisation in Inheritance Law

The paper *“The Impact of Digitalisation in Inheritance Law”* by Akramov, Rakhmonkulova, Khazratkulov et al.[4] explores how digital legacy is changing perceptions about inheritance. As more people hold digital assets like cryptocurrencies, social media profiles, and online accounts, traditional inheritance systems are starting to fall behind. The authors approach the issue from a technical perspective, aiming to propose a framework that can help address the new challenges that come with managing digital legacies.

One of the issues discussed is how aspects like access rights, ownership, and privacy becomes complex as they starts to cover digital assets. The paper uses real-world examples, like the case of Gerald Cotten, CEO of Quadriga (cryptocurrency exchange), who died without sharing access to an estimated \$190 million, according to the paper, in digital currency. This example is used to underlined consequences associated with the lack of post-mortem planning[4].

The paper addresses the risks around digital will documents created and stored electronically. While digital wills can make estate planning more accessible, they also cause security concerns. Wills can be copied, edited, or hacked. This sets higher requirements for what system currently offer in protection of digital wills. The authors points out that existing platforms rely on weak verification methods, encryption and access controls.

A point throughout the paper is that international rules and standards are still lacking. With digital assets often being stored online across different countries, the absence of clear global regulations creates confusion and legal risks. The authors also raise the concern that NOK might gain access to private information that the deceased never intended to share, which raises important ethical questions.

Summary of reviewed literature

Altogether, the reviewed literature shows that digital death is no longer just an ethical question. While most users have not made concrete plans for what happens to their digital legacy, there is growing awareness of the need for tools and systems that can support digital legacy management. The studies highlight different aspects of the problem: From user expectations and emotional barriers, to the technical and legal challenges of building secure and respectful digital legacy services. Whether it is through centralised services, user-friendly security tools, or culturally sensitive system design, there is a clear demand for more thoughtful approaches to digital legacy management. The existing research lays the foundation for reimagining how death is handled in the digital space and aligns closely with the aim of the thesis of exploring more thoughtful, user-centered approaches to managing digital legacy, as stated in section 1.2.

3.2 Existing commercial solutions

In the field of digital legacy management, a number of commercial solutions have emerged in recent years, each addressing different aspects of what happens to the metasoul of users after death. These platforms can be grouped into three categories:

- **Digital estate and testament handling:** Services that help users create digital wills and choose legacy contacts for digital assets (e.g. CloCr[8], Final Security[32])
- **Access control and inheritance services:** Services that store password and digital assets for secure transfer after death (e.g. Inheriti[45], My-Legacy.ai[58], Vault12[82])
- **Automated account deletion or privacy cleanup tools** Services that help users delete the digital footprint before or after death (e.g. DeleteMe[18])

CloCr

CloCr is a combined digital legacy and testament management service. It allows users to upload, encrypt, and organise key documents such as wills, letters of instruction, account credentials, as well as designate trusted NOK that gains access upon verification of the death or incapacity of the user. CloCr emphasises their implementation of end-to-end encryption and chain of custody safeguards, and offers a guided tool for building a will.[8].

Final Security

Final Security offers a broader digital legacy management that includes not only secure storage of credentials and legal documents, but also a repository for social media legacy content. After the passing of a user, designated NOK can access a curated *memory box* containing messages, photos, and videos. The platform integrates identity verification

steps to guard against wrongful access, and provides one-on-one support for both account setup and post-mortem release processes.[32].

Inheriti

Inheriti takes a two part approach, combining secure vault storage for digital passwords and assets with a “*backup and release*” schedule that automatically hands off cryptographic keys to designated NOK. It is particularly aimed at users who maintain extensive cryptocurrency holdings or cloud-based file archives, providing API integrations with major wallets and storage services. Compliance with the GDPR ensures that users in the EU can trust that their personal data is processed transparently, securely, and in accordance with their rights, and it gives users confidence that their privacy is respected and that they remain in control of their own information.[45].

My-Legacy.ai

My-Legacy.ai focuses on access control and automated message delivery. Users record video or audio messages to be sent to loved ones at pre-specified times, alongside the secure storage of passwords and documents. Its AI-driven interface can suggest “*legacy messages*” based on the handwriting samples and speech patterns of the user, adding a personalised tone to their post-mortem communication with NOK. These services gives users the opportunity to live on digitally through their communication features[58].

Vault12

Vault12 focuses on decentralised key storage, rather than holding encrypted vaults on central servers, it shards the private keys of users among a distributed network of “*guardians*”, trusted friends or devices. In the event of the death of a user, “*guardians*” can collaborate to reassemble the keys and grant NOK access. This design reduces single point-failure risk and support privacy, since no single server ever holds the full decryption key[82].

DeleteMe

DeleteMe approaches digital legacy from the opposite angle, rather than passing assets on, it allows users to proactively remove their personal data from service providers. Its service includes automated takedown requests, regular monitoring of data aggregators, and secure reports confirming removal. Although not a digital legacy management service in the traditional sense, DeleteMe addresses the concern that unwanted data lives on indefinitely after the death of a user[18].

Chapter 4

Methodology

This chapter outlines the methodologies applied in the threefold research of legal frameworks, service providers, and empirical data, as well as the design and development of the UPAP .

4.1 Legal Frameworks

In order to understand how digital legacy is shaped by law, this thesis includes an exploration of the legal frameworks that focus on how personal data is treated after death within the Scandinavian countries and briefly touches on China's policies. The goal of this part of the methodology is to explore which legal frameworks currently exist, what gaps they leave behind, and how they support or obstruct the development of digital legacy management systems.

This part of the research is qualitative and interpretive in nature. Legal texts were examined across multiple jurisdictions, including the General Data Protection Regulation (GDPR)[34] and its national implementations in Denmark, Sweden and Norway, as well as China's Personal Information Protection Law (PIPL)[63].

The comparative reading was guided by the following set of questions:

- Does the law offer protection for the data of deceased persons?
- Can next of kin gain access to digital accounts or files?
- Are there specific procedures or rights for managing digital assets post-mortem?
- Is post-mortem assets regulated through data protection, inheritance law, or terms of service?

Legal materials were sourced from official legal resources, including government websites, academic papers, national data protection authorities and existing legal commentary.

4.1.1 Denmark & other Scandinavian countries

Denmark serves as the central point of reference for this research as the primary thesis scope is focused on how Danish regulatory frameworks approach digital legacy management. This starting point ensures the research relevance and applicability within a Danish context. However, to achieve a comparative exploration, additional countries and European initiatives have been selected based on their similarity to Denmark. According to the Digital Economy and Society Index (DESI)[24], Norway and Sweden consistently rank highly, indicating advanced digital economies and similar societal attitudes towards digital privacy and data management.

4.1.2 China's Personal Information Protection Law (PIPL)

The focus on China's Personal Information Protection Law (PIPL) was inspired by an interview with a privacy engineering lecturer at Aalborg University (AAU), where it was discussed as a contrasting perspective to Europe's GDPR. An overview of the interviews can be found in Table 4.2.

After initial research, China appeared as a country with consistently low scores on privacy indices[5, 21, 65], often cited for extensive governmental surveillance and limited individual protections.

Furthermore, studies indicate that China's privacy laws do not truly limit state surveillance but are used to make the government appear protective by targeting private companies and local authorities.[48]

Although China's approach to privacy laws might differ from Denmark and the European Union (EU), PIPL was included in the research. This decision was based on the different approach of PIPL regarding post-mortem data rights in comparison to GDPR. Furthermore, this raised questions in the discussion about how a country ranking low on multiple privacy indices would account for post-mortem data management.

4.1.3 European regulatory frameworks for digital governance

4.1.3.1 eIDAS 2.0 & Digital identity infrastructure

eIDAS 2.0 (Electronic Identification, Authentication and Trust Services) is included as it adds a different perspective to the digital legacy landscape. As digital legacy management involves sensitive data, verified access, and identity delegation, eIDAS 2.0 provides a relevant legal and technical framework for understanding how identity authentication could function across European borders in a post-mortem context. Its inclusion helps

situate the thesis within current developments in European digital infrastructure and allows for discussion of how such frameworks may support or challenge digital inheritance practices.[25, 76]

4.1.3.2 European Law Institute (ELI)

A project from European Law Institute (ELI), *ELI Succession of Digital Assets, Data and other Digital Remains*[29], that describes the succession of digital assets, was including the legal research, due to its aim of establishing harmonised guidelines for handling digital legacies across the EU.

The project is relevant to this thesis as it directly addresses post-mortem data rights, access issues, and cross-border inheritance challenges. Including this project helps connect the thesis to current legal explorations and proposals on digital inheritance within the European context.[29, 46]

4.1.3.3 Digital Services Act (DSA) & Digital Markets Act (DMA)

The Digital Services Act (DSA) and Digital Markets Act (DMA) are included in this thesis as part of the broader regulatory environment affecting digital platforms in the EU. Although not focused specifically on digital legacy, these acts influence how data is managed, accessed, and transferred between users and services. Their inclusion supports the thesis goal of evaluating the current policy landscape and understanding the structures that shape how digital identity and personal data may be handled after death. [27, 28, 30, 50]

4.2 Service Providers

As part of this thesis, an objective is to understand how current digital platforms handle the management of user data after death. An analysis was conducted on a selection of service providers across different sectors, presented in Table 6.1, with the goal of identifying their current standard for supporting post-mortem account handling. The findings from this analysis were used to guide the design considerations for the proposed solution UPAP, described in chapter 9.

The method used was qualitative and descriptive in nature. A spreadsheet was developed to systematically collect and organise policy information. The service providers selected include those that are commonly used in everyday life: social media networks[6], email and account services, financial platforms like crypto exchanges[11], and gaming services. The rationale behind this variety was to represent a broad spectrum of digital identity types, from communication and content storage to financial and entertainment-related accounts. This reflects the increasingly diverse nature of modern digital footprints.

The spreadsheet includes details that directly relate to the ways service providers handles digital legacy management. The details included is the following:

- Whether the provider has an official post-mortem policy.
- Availability of account deactivation, deletion, or memorialisation procedures.
- How inactivity is handled, and whether it leads to automatic suspension or deletion.
- The level of default access granted to NOK or potential third parties.
- Whether users can proactively assign legacy contacts, while the user is still alive.
- The procedural steps required for both pre-mortem planning and post-mortem access, such as the need for death certificates, legal proof of authority, or other documentation.
- The types of actions NOK are allowed to perform after the death of the user (e.g., deleting content, downloading data, managing friend requests, receiving funds, etc.).

To populate the spreadsheet, the primary source of information was the official policy documentation or help center pages of each provider. When policies were incomplete, unclear, or not available, secondary sources such as community forums, unofficial FAQs, and support threads were utilised. These “*unofficial resources*” were clearly marked in the dataset, in Table 6.2, and used cautiously, serving mainly to highlight policy gaps or inconsistent practices across platforms.

By mapping out this information in a structured way, the analysis helped identify differences in how service providers handle data of the deceased and revealed common weaknesses, limited user control, and inconsistent processes. This supports the research goal of this thesis, which is to explore how digital legacy systems can be designed in a more user-centered, ethically sound, and technically feasible way.

This methodology serves as an foundation for the proposal of a proof of concept (POC) UPAP, described in chapter 9. By identifying not just what is missing but also what is available in current practices, this analysis helps bridge the gap between user expectations, that was identified in section 7.1 and section 7.2, and the options for metasoul management with service providers.

4.2.1 Service Provider Data Analysis

To facilitate the analysis of the approaches of service providers in regards to post-mortem data management, the spreadsheet data was exported in CSV (comma-separated values) format and uploaded to Google Colab[36], an in-browser platform that supports Python code execution without requiring local installation. Google Colab was chosen for its collaboration features and the flexibility to rerun analyses as the dataset was updated.

For data cleaning and normalisation, column names were standardised and translated from Danish to English to ensure consistency throughout the analysis. This involved removing unnecessary spaces, converting all text to lowercase, and replacing or removing special characters.

Where possible, data values were normalised. Boolean fields, time periods, and access levels, ranging from *no access* to *full access*, were converted into consistent formats. Open-ended responses were retained in their original form, as the dataset was comprised of 140 respondents with only a subset of those using open-ended responses. This allowed for manual review and interpretation.

4.3 Data Collection

4.3.1 Quantitative Survey

This section describes how the survey was developed, distributed, and carried out to explore how people in Denmark relate to the topic of digital legacy. The survey aimed to get a better understanding of the general level of awareness about digital legacy, personal experiences with managing digital data after death, and the actions or preparations that respondents have taken to manage their own digital legacy. It also focused on attitudes towards ownership of digital assets, the role of digital guardianship, and planning for digital financial assets in the form of cryptocurrency.

To address these themes, a quantitative survey was selected as the method for data collection. The survey design was inspired by elements from the work of Maciel et al. in "*Defining Digital Legacy Management Systems' Requirements*".[53] Their framework was used to identify relevant areas and question types that focus on the perspectives of users, including what actions people have taken to manage digital legacy both before and after the loss of a relative.

The survey consisted of 20 questions, divided into seven sections:

| |
|--|
| <p>Background information</p> <ol style="list-style-type: none"> 1. What age group do you belong to? 2. What is your occupation? 3. How digitally dependent would you say your everyday life is? 4. Do you use social media? <ol style="list-style-type: none"> 4.1. If yes, how many different platforms are you a member of? |
| <p>Understanding and attitudes towards digital legacy</p> <ol style="list-style-type: none"> 5. Do you know what digital legacy is? <ol style="list-style-type: none"> 5.1. If yes, how would you define it in your own words? 6. Have you ever thought about what happens to your digital data after your death? 7. To what extent do you think it is important to consider your digital legacy? 8. What consequences do you see in not considering your digital legacy? |
| <p>Personal experiences with others' digital data</p> <ol style="list-style-type: none"> 9. Have you ever had to handle a deceased person's digital data? <ol style="list-style-type: none"> 9.1 If yes, what challenges did you experience? 10. If a loved one passed away, how would you handle their data? |
| <p>Measures and solutions taken for one's own digital legacy</p> <ol style="list-style-type: none"> 11. Have you taken any specific measures? <ol style="list-style-type: none"> 11.1. If no, what has prevented you? 12. Would your next of kin have access to your important digital accounts if something were to happen to you? 13. Do you read terms and conditions regarding digital legacy? 14. If you could plan your digital legacy, which of the following would you prefer? 15. For each of the following platforms, how would you like your account to be handled after your death? <i>Note: Five service providers were included with 4 options for handling; transfer, keep, delete, no account</i> 16. How do you feel about a "digital guardian"? |
| <p>Views on ownership and rights to digital content</p> <ol style="list-style-type: none"> 17. Who do you think has the right to decide over your digital accounts when you are no longer here? 18. In your opinion, who owns your digital assets (e.g., photos, messages, videos) after your death? |
| <p>Cryptocurrency</p> <ol style="list-style-type: none"> 19. Do you own any cryptocurrencies? <ol style="list-style-type: none"> 19.1. If yes, have you made a plan for what should happen to them if you pass away? 19.2. If you died today, would your family know how to access your important digital accounts? |
| <p>Final reflections and comments</p> <ol style="list-style-type: none"> 20. Do you have any additional comments or thoughts about the topic of digital legacy and handling data after death? |

Table 4.1: Overview of questions included in quantitative survey

The survey was created using Fillout[31], a forms and survey builder, which made it possible to combine multiple question types in a user-friendly format. The majority of questions were multiple choice, often with two to five predefined options. The full list of questions and their answers is available in Appendix C.

Some questions included the option to provide a written explanation in an open-ended response, which introduced a qualitative nature to the survey. However the survey is primarily based on questions of quantitative nature. This allowed respondents to add personal reflections. The questions was prepared with the intention of gaining insights into the experiences of respondents with handling digital legacy data and how they would prefer their own digital content to be handled.

The questionnaire was distributed by sharing the survey link on LinkedIn and Facebook. These platforms were chosen to reach a wide and varied demographic, including younger digital users, working professionals, and older adults with the potential exposure to digital legacy management. The survey remained open for responses from 20 February to 25 March 2025, during which 140 respondents submitted their response.

Participation in the survey was voluntary and anonymous. Respondents were informed that they could choose to provide their email address at the end of the survey if they were interested in being contacted for a possible follow-up interview, which resulted in the selection of some respondents for further interview, described in section 7.1.

This approach provided a structured way to collect data on how individuals in Denmark perceive and manage their digital legacy. The use of a standardised online survey format ensured consistency across responses, while the open-ended elements gave respondents space to add nuance to their answers.

4.3.1.1 Survey Data Analysis

The quantitative survey was designed and distributed in the Danish language to ensure accessibility and ease of understanding for the targeted audience. As the responses were collected in Danish the dataset was translated into English and the survey variables standardised. These steps ensured consistency in naming conventions, supported accurate script development in Google Colab[36], and enabled clearer interpretation of results.

For example, the question "*Hvordan ville du håndtere en nærtståendes digitale data efter deres død?*" was mapped to the variable `handle_loved_ones_data`. The corresponding response values were also translated and standardised. Below is a snippet showing how this was handled:

```
df['handle_loved_ones_data'] = df['handle_loved_ones_data'].str.replace(
    'Jeg ville forsøge at lukke deres konti.', 'Close accounts', regex=False)
```

This line replaces all exact occurrences of the Danish string "*Jeg ville forsøge at lukke deres*

konti." in the `handle_loved_ones_data` column with the standardised English label "Close accounts".

Most of the multiple-choice questions were visualised using bar charts, with the number of respondents on the y-axis and the answer options on the x-axis. Absolute numbers were preferred over percentages, as the overall number of responses was limited. This approach was relevant for sub-questions aimed at smaller respondent groups, such as cryptocurrencies holders.

To quantify user responses, most survey questions were structured as closed-ended multiple-choice items. While no formal Likert scale (e.g., 1–5 or 1–7 agreement levels) was applied, several questions presented categories that could be mapped to a graded responses. For instance, digital dependency was expressed through a four-point scale ranging from *I use digital solutions for almost everything* to *I avoid them as much as possible*. These scales were treated as categorical variables in the analysis.

For the analysis of the survey data, Google Colab was again employed for the same reasons outlined previously, in section 4.2. This ensured a consistent and collaborative workflow, particularly as survey responses were collected and processed continuously.

In Python, the `pandas` library was used for data manipulation and analysis, with `matplotlib` and `seaborn` supporting the creation of visualisations.

4.3.2 Qualitative Interviews

To better understand the practical and emotional implications of digital legacy management, a series of semi-structured qualitative interviews were conducted. The aim of this phase was to explore individual and organisational experiences with accessing or managing digital data after the death of a person and to learn how existing systems support or fail to support such processes.

The interviews followed a set of preformulated questions, listed in Appendix A, which served as a flexible guide rather than a strict script. This allowed the conversations to remain open-ended and adaptive to unique experiences for each participant. Each interview began with a short presentation of the thesis, ensuring participants understood the context and how their input would be used. All participants were informed about citation and identification, giving consent, and reviewing the parts where they were mentioned.

The selection of participants was based on relevance and first-hand experience. The individuals interviewed are presented in Table 4.2.

| Interviewee | Relevant focus |
|--|--|
| Johan Niordson, IT-lead and surviving spouse | Close family member who managed digital accounts after the death of his spouse in Denmark. |
| Sakariye Ali, Software engineer and son | Experienced legal barriers managing digital accounts after a Danish family member died in Somalia. |
| Bilal B., Head of IT support, and Janni B., CISO, University of Southern Denmark (SDU) | Involved in handling digital accounts and internal procedures following the death of employees or students |
| Astrid Waagstein, PhD in post-mortem data rights | Domain expert and researcher with long-term focus on ethical, legal, and technical aspects of digital death. |
| Privacy engineering lecturer, Aalborg University (AAU) | AI ethics, privacy design and data control |

Table 4.2: Overview of qualitative interview participants

The interviews were selected to provide a balanced perspective, including two based on personal experiences, two with experts, and one with an organisation offering insight as a neutral party in handling digital legacies.

The interviews aimed to gather both technical insights, such as how data access is granted or restricted, and emotional reflections on the current processes. Topics included MitID[57] shutdowns, legal recognition of death certificates, access to e-Boks[22], account management, organisational workflows, and emotional reactions to digital inaccessibility.

All conversations were documented through note taking during or immediately after the interviews. No audio or video recordings were used, as the aim was to create a respectful and emotionally sensitive setting, given the personal nature of the topic. This approach was chosen to minimise intrusion and provide a more comfortable environment for interviewees sharing experiences related to death and digital legacy. Further details are provided in subsection 10.2.3.

The qualitative interviews provides a grounded perspective on how real users and organisations navigate the gaps between law, technology, and grief. It complements legal framework exploration, described in chapter 5, by adding lived experience to the legal frameworks. The interview data was used to highlight common friction points and emotional aspects that current systems overlook.

4.4 Proposal of a proof of concept

This thesis includes the design and development of a protocol for service providers named UPAP.

UPAP aims to help service providers manage digital assets and user accounts after the death of a user in a secure, respectful, and practical way. The design of UPAP includes the needs of user and their NOK, reflect on legal frameworks in its implementation, and create a solution that service providers could realistically implement.

4.4.1 Evaluating architectural approaches

Before the design of UPAP, the importance of how digital legacy management responsibilities is distributed was recognised. To guide this decision, a workshop was organised internally in the group in which two possible models were compared: a centralised solution, managed by one or more third-party authorities, and a decentralised solution, managed individually by service providers. A table of pros and cons, available in section 9.4, was created, evaluating both models across five criteria: *Security*, *Compliance*, *User experience*, *Cost efficiency*, and *Death verification*.

4.4.2 Workshop process and protocol design

To ensure that UPAP would be both effective and practical, a collaborative workshop by the group was conducted and performed in a collaborative Miro board[56], an online whiteboard. This helped organise and visualise the outputs of the workshop. The workshop aimed to answer the following themed questions:

- **Problem definition and scope:**
 - To define the problem space, the process began by identifying gaps in current post-mortem data management practices. The types of digital assets to be included were mapped, and potential jurisdictional challenges were outlined.
- **Core principles and compliance:**
 - Relevant legal frameworks were reviewed to establish baseline compliance requirements. Particular attention was given to balancing privacy for the deceased with NOK access, and an evaluation of whether default actions should involve deletion or transfer of data.
- **Technical architecture:**
 - To form the system design, different methods for reliable death verification were explored. Service providers were categorised in severity levels based on the data they hold, and the consequences of misuse or unauthorised access to the

account. Authentication methods for NOK were assessed, alongside integration possibilities with service provider.

- **User workflow and features:**

- User flows were modelled using sequence diagrams to outline how users delegate access, set their preferences for post-mortem handling, and how NOK could be designated and authenticated. Requirements for metadata accompanying digital assets were defined, and procedures for stakeholder notifications and death verification were mapped. Feature specifications were derived from these workflows.

- **Outlining validation and evaluation metrics:**

- A set of evaluation metrics were established to guide the future assessment of the protocol. These should include accuracy of death verification and usability for users and NOK. Furthermore a list of possible ethical risks such as privacy violations and misuse were outlined. As stated in section 1.2, this thesis will only outline relevant evaluation metrics. No validation or testing will be performed.

The design of UPAP is carried out and described in chapter 9.

Chapter 5

Exploration of Legal Frameworks

This section aims to explore and compare how different legal frameworks govern the protection of personal data after death, with the primary focus on Danish Data Protection Act[49], *Databeskyttelsesloven*, as it supplements the General Data Protection Regulation (GDPR).[34]

The exploration includes insights from Denmark's neighbouring and fellow Scandinavian countries, Norway and Sweden. Furthermore the exploration examines how the GDPR governs protection of personal data after death with a comparison to China's Personal Information Protection Law. Finally, the exploration examines relevant initiatives from the European Union. The basis for the selection of the scope of this exploration is described in section 4.1.

The exploration focuses on legal rulings, access rights and inheritance laws for NOK, and whether individuals can determine the post-mortem fate of their personal data. The exploration examines the following in the order listed below:

- Primarily focused on Denmark with insights from:
 - Danish Data Protection Act (*Databeskyttelsesloven*)[49]
- Exploration of General Data Protection Regulation (GDPR)[34]
- Comparison with China's PIPL[63]
- Comparison with other Scandinavian countries
 - Norway's Personal Data Act (*Personopplysningsloven*)[55] and Norway's Data Protection Authority (*Datatilsynet*)[79]
 - Sweden's Data Protection Act (*Integritetsskyddsmyndigheten*)[47] and Tax Agency (*Skatteverket*)[55]

- Exploration of relevant EU initiatives
 - eIDAS 2.0 Regulation (*Electronic identification, authentication and trust services*)[25]
 - European Law Institute (*Succession of digital assets project*)[29]
 - Digital Markets Act (DMA)[27]
 - Digital Services Act (DSA)[28]

5.1 Danish Data Protection Act

In Denmark, specific provisions extend data protection to deceased individuals. According to §2, subsection 5 of Danish Data Protection Act[49], the GDPR applies to the personal data of deceased individuals for a period of ten years following their death. Subsection 6 further provides that the Minister of Justice, after consultation with the relevant minister, may establish regulations stating that the subsection and thereby GDPR should apply to the individual for a period either longer or shorter than the ten years specified in subsection 5.

5.2 GDPR and PIPL

5.2.1 GDPR

Under the GDPR, Recital 27 explicitly states that the regulation “*Does not apply to the personal data of deceased persons*”. This means that once a person has passed away, the GDPR no longer offers any protection over their personal data. However, it allows each EU Member State to create their own national laws about how data is handled after death.[35]

In the absence of a unified EU-level regulation, legal uncertainty may arise, especially in cross-border situations where multiple jurisdictions are involved. Moreover, it raises ethical concerns about digital dignity, referring to respecting the online identity, privacy, and legacy of a deceased person, and the management of sensitive information, such as social media accounts or cloud storage, after death.

5.2.2 PIPL

As mentioned in chapter 4, China was included in the exploration of legal frameworks, as it represents a different approach to digital privacy and the handling of individual rights post-mortem.

In contrast to the GDPR, China’s PIPL, Article 49[62], introduces a more explicit approach. Article 49 allows NOK to exercise certain data rights over the personal information of the deceased. These rights include the ability to access, copy, correct, or delete data, provided

that doing so is in the lawful and legitimate interest of the surviving family members. However, this applies only if the deceased did not leave instructions prior to their death.

This part of the law is based on the idea that privacy does not end with death and that the data of a person can still affect their family and close relations. It gives families some degree of authority and responsibility in managing the digital legacy of the deceased.

5.2.3 Comparative evaluation between GDPR and PIPL

The protection of personal data for deceased individuals represents a significant point of divergence between the General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL). Both legal instruments aim to establish high standards for privacy and data protection, but their approach to post-mortem data rights differs fundamentally, as the GDPR clearly states, its protections stop when a person dies. This comparison raises the question of how China, despite its different approach to privacy, still acknowledges post-mortem rights, something the GDPR does not.

5.3 Scandinavian context

5.3.1 Norway

Norway, despite not being a member of the EU, is bound by the GDPR through its membership of the European Economic Area (EEA).

However, Norwegian legislation extends[55] the scoping of the GDPR and does not apply to individuals post-mortem.

Despite this scoping, the Norwegian Data Protection Authority, *Datatilsynet*, addresses post-mortem management in an employee context. It states that information that concerns a deceased person and simultaneously identifies living individuals, is still regarded as personal data of the living and remains protected under privacy laws.[13]

The Norwegian Data Protection Authority, *Datatilsynet*, [13] also provides specific guidance on how employers should handle personal data of deceased employees. The employer has a legal obligation to evaluate personal data that should be deleted after the death of an employee. Central to this process is the personnel card[14], a document that the employee is encouraged to complete during their employment. This card instructs employees to separate private and work-related data and to clearly label private folders. Moreover, the personnel card allows employees to make practical agreements with their employer regarding post-mortem data handling. However, such agreements are purely organisational and do not constitute valid legal consent.

If no personnel card is prepared, the general rule is that no access is granted to NOK, and the employer must delete private data without review. There is no automatic right of

access for relatives and the employers must carefully balance the privacy of the deceased against operational needs and risks before considering sharing private data.[14]

Under the GDPR, individuals have rights only to their own personal data. This means that relatives do not automatically have the right to access the data of a deceased person. If the data of the deceased contains information about living persons, for instance, information about relatives in private documents or colleagues in email correspondence, employers must consider whether disclosure could endanger the privacy of other persons.

Furthermore, when accessing the data of the deceased for operational reasons, employers are bound by strict limitations:

- Email accounts must be closed and deactivated unless business-critical information needs retrieval.
- Only data necessary for business continuity may be accessed.
- Before accessing, the employer must evaluate whether alternative, less intrusive options exist, such as:
 - Retrieving information from colleagues.
 - Forwarding specific business-related emails without opening entire mailboxes.
- Access must be targeted and limited to relevant content.
- Clearly marked *PRIVATE* areas must never be accessed, even when business reasons justify reviewing other data.

It is recommended that a union representative or an independent observer participate in the process when accessing personal data to ensure transparency and respect for privacy.

In summary, while the Norwegian Personal Data Act[55] allows a practical framework for managing the digital assets and personal data of the deceased, it also recommends that employers and NOK protects the rights of living individuals and acts with caution, respect, and considers necessity when handling sensitive post-mortem data.

5.3.2 Sweden

The legal insights of Sweden is based on the Swedish Tax Agency (*Skatteverket*)[72] and the Swedish Data Protection Act (*Integritetsskyddsmyndigheten*)[47].

According to the insights, the GDPR does not apply to deceased individuals in Sweden. Although Sweden has specific laws that regulate the handling of data about deceased persons in certain areas, such as the Population Registration Act (*Folkbokföringslagen, FdbL*)[33] and the Tax Data Act (*Skattedatalagen, SdbL*)[71], these laws only cover limited contexts like information about population registration and taxation.

5.4 European initiatives

5.4.1 The role of eIDAS 2.0 in digital legacy management

An aspect of this exploration has been to explore how emerging EU regulations on digital identity, particularly the eIDAS 2.0 regulation, may support the future handling of digital legacy. Managing digital legacies involves sensitive information, identity verification, and often legally binding processes after the death of an individual, all of which require a trustworthy and interoperable framework.

To address these growing needs, the European Commission[25] introduced eIDAS 2.0[25], which expands the scope of the regulation, initially established in the first edition of eIDAS[20]. A central element is the establishment of the European Digital Identity Wallet[26], which is a secure and user-controlled solution for storing and sharing personal credentials online. This wallet could play a significant role in future digital legacy management by allowing individuals to securely store post-mortem instructions, identity-linked permissions, and other relevant legal documents.

This research reviewed official documentation[80] and academic commentary[76] to assess the relevance of eIDAS 2.0 in digital legacy management. Notable aspects include:

- **Verified identity access:** Strong identity assurance levels help confirm who should be granted access to the digital accounts or data of a deceased individual.
- **Cross-border compatibility:** With digital assets often held across jurisdictions, the mutual recognition of digital signatures helps reduce legal ambiguity.
- **User consent and control:** Emphasising user consent aligns well with ethical considerations around data handling after death.
- **Trust services for post-mortem actions:** Services like storage services could ensure the integrity of wills or post-mortem data permissions.

Although the regulation does not explicitly focus on post-mortem data management, its components offer valuable infrastructure for future systems dealing with digital inheritance and access control. This makes eIDAS 2.0 a meaningful reference point when considering how digital legacy management could be supported by secure and recognised frameworks across Europe.

5.4.2 Review of European Law Institute (ELI) on digital inheritance

In order to further understand the legal field surrounding digital legacy management, this thesis also includes an exploration of the new project, of European Law Institute (ELI), titled *“Succession of Digital Assets, Data, and Other Digital Remains”*. [29]

The project builds on management of digital assets across Europe, but specifically focuses

on what happens to the digital presence of an individual after death, including ownership rights, access permissions, and succession planning. The project, announced in October 2023 by ELI, aims to harmonise and clarify the rules and principles that govern the transfer of digital assets in cases of death. While digital inheritance has been partly addressed by national regulations and private initiatives, a cross-border approach has so far been missing. The recent work of ELI seeks to fill this gap, offering guidance for national legislators, notaries, lawyers, and service providers that manage user accounts.

Elements from the review include the recognition of digital assets as inheritable property. ELI highlights that digital assets, such as cryptocurrencies, social media accounts, and cloud-stored files, should be treated as part of the estate. However, varying national definitions of “*property*” complicate matters, particularly for assets that do not fit easily into traditional legal categories.

A list of recurring obstacles addressed by ELI:

- **Conflict of laws and jurisdiction issues:**
Many digital assets are stored, by platforms, across borders. The ELI project emphasises the need for clear rules on applicable law, as inconsistent approaches can stall or invalidate succession procedures.
- **Role of contracts and user agreements:**
There is often a conflict between inheritance rights and platform terms of service that prohibit account transfer. ELI argues that legal frameworks must either override or align with these agreements to balance user rights and provider policies.
- **Privacy and post-mortem data protection:**
Inherited digital assets can include sensitive data like emails or photos, potentially affecting the privacy of the deceased and third parties. The project raises ethical and legal concerns about whether, and how, NOK should access such data.

5.4.3 Fairness and responsibility in the EU digital space

5.4.3.1 The Digital Markets Act: Reining in the gatekeepers

The Digital Markets Act (DMA) is meant to prevent large tech companies from taking unfair advantage of their position. One important rule is that they have to let users move their data between different services and make their systems work with others.[27] For digital legacy management, this could allow individuals or their NOK to retrieve data from one of these EU identified gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft and either transfer it to another, preserve it, or request its deletion. This helps address current problems where NOK must go through fragmented and unclear processes across multiple service providers, as described in chapter 6.

Another relevant rule is the ban on self-preferencing, which ensures that any of the EU

identified gatekeepers cannot prioritise their own services in ways that block smaller competitors including those offering digital inheritance solutions. This could encourage a more diverse ecosystem of digital legacy management services. Though these laws do not yet offer direct solutions to post-mortem data issues, they open up new regulatory space for future legislation. They also give users more leverage over their digital presence during life and potentially after death.

5.4.3.2 The Digital Services Act: More transparency, more accountability

The Digital Services Act (DSA) is largely focused on increased responsibility among online platforms when it comes to content moderation, illegal material, and user safety. One of the central goals of the DSA is to increase transparency in platform operations. Under the regulation, especially for bigger online platforms, there are new obligations to explain how content is recommended, removed, or down-ranked. Additionally, users are to be provided with clearer channels for appealing moderation decisions.[30]

Although the DSA does not specifically address post-mortem data, its emphasis on how platform transparency should look in the future, support clearer processes for families or legal representatives. This might include better insight into what content remains online after the death of an individual, what has been removed, and how to contest platform decisions if needed.[30]

For the first time, systemic risk assessments are required from the largest tech companies, firms the size of Microsoft, Meta, and Google[27], including how their services might impact public discourse or mental health. There is potential for future interpretations to address how death legacies is managed, particularly regarding the emotional burden placed on grieving families by the continued algorithmic visibility of the deceased.[50]

As part of the EU's broader strategy for a *Europe fit for the digital age*, the DSA and the DMA were introduced to rebalance the relationship between large service providers.[27] While these laws do not directly regulate post-mortem data, they reshape the broader ecosystem that governs how digital identities and personal data, including digital remains, are stored, accessed, and protected.

Chapter 6

Analysis of Service Providers

This section explores how different online service providers approach digital legacy and post-mortem data management. A total of 20 providers were selected for analysis, spanning eight categories that reflect diverse aspects of digital life. These include social media platforms, email providers, account services, financial platforms, and tools for communication, entertainment, and security. Table 6.1 below presents the full list of providers included in the analysis, grouped by service type.

| Category | Service Provider |
|-------------------|-------------------|
| Social Media | Facebook |
| | X (Twitter) |
| | LinkedIn |
| | Instagram |
| | TikTok |
| | Snapchat |
| | Reddit |
| Mail Provider | Microsoft Outlook |
| Crypto Exchange | Coinbase |
| Gaming | Steam |
| Entertainment | Netflix |
| Account Services | Google Account |
| | Apple Account |
| Communication | Signal |
| | WhatsApp |
| | Discord |
| Password Managers | Bitwarden |
| | SecureSafe |
| | NordPass |
| | 1Password |

Table 6.1: List of analysed service providers by category

These eight categories were selected to provide a broad perspective on the range of digital platforms in use today, reflecting the way digital legacies extend across multiple services and account types. The selection is described in more detail in section 4.2.

The selected service providers represent a diverse cross-section of the digital ecosystem, each with unique implications for digital legacy.

Social media platforms were included due to their widespread use and the large volume of personal data they host. Email providers and account services were selected because they serve as central authentication nodes, offering recovery access to numerous other services and accounts. Communication apps store large volumes of personal and intimate content, including messages, media, and real-time interactions, which are tied to the private aspects of the digital footprint of the user. A crypto exchange was included for their legal and financial complexity, as it represent a form of digital financial inheritance. A gaming platform is included as users accumulate digital ownership of games and in-platform assets. Finally, password managers were selected for their critical role in access control, as they serve as central vaults for login credentials throughout the digital life of a user.

The analysis is based primarily on the official and publicly policies of each service provider.

The focus is on how providers handle post-mortem management, including procedures for deactivation, deletion, and possible transfer of account access. When available, official documents were used from the official websites of the providers. These documents address post-mortem handling directly.

If direct official policies were not available, secondary resources were used. These include support ticket responses and help pages from the website of the provider. Some of these pages discuss related topics, such as account inactivity or general account management.

For service providers without official policies or relevant support documentation, third-party sources such as guidelines from communities were used as basis when no other options were available. The resources are used with their limitations in mind during the analysis. No service providers were contacted during the analysis.

The following overview presents the service providers and titles of the resources referenced in this analysis. Resources are grouped into three types:

1. Official documents from the website of the provider about post-mortem handling,
2. Secondary resources that discuss the topic indirectly,
3. Third-party sources, used only if official or secondary resources were not available.

This approach ensured a systematic review of post-mortem account management across major digital service providers as of May 18, 2025.

6.1 List of Service Provider policy resources

| Service provider | Ressource | Policy description |
|-------------------|-------------------------|--|
| Google Account | Official | Submit a request regarding a deceased user's account[77] |
| Microsoft Outlook | Official | Accessing Outlook.com, OneDrive and other Microsoft services when someone has died[3] |
| Apple Account | Official | How to request access to a deceased family member's Apple Account[42] |
| Whatsapp | Secondary | About inactive account deletion[1] |
| Signal | Secondary | Delete Account[17] |
| Discord | Official | Deceased or Incapacitated Users[16] |
| Coinbase | Official | Claim a decedent's Coinbase account[7] |
| Netflix | Official | How to cancel an account for a deceased Netflix member[40] |
| Steam | Secondary | Steam Subscriber Agreement[73] Account Deletion - Common Questions[74] Providing Proof of Ownership[75] Privacy Policy Agreement[64] |
| Bitwarden | Official | Emergency Access[23] |
| SecureSafe | Official | Data Inheritance: How It Works and Why It Matters[12] |
| NordPass | Official | Introducing a New Feature — Emergency Access[59] |
| 1Password | Official | The complete guide to digital estate planning, Get to know your Emergency Kit[78] |
| Facebook | Official | Request to Memorialise or Remove an Account[69] |
| X (Twitter) | Official | How to contact X about a deceased family member's account[9] |
| LinkedIn | Official | Deceased LinkedIn members[15] Create a memory profile or close the account if a member has passed away[10] Request to close a deceased member's LinkedIn profile[68] |
| Instagram | Official | Report a deceased person's account on Instagram[67] |
| TikTok | Third party | How To Delete A Loved One's TikTok Account[41] |
| Snapchat | Secondary & Third party | I'd like to report an account of a person who passed away[43] Dealing with social media accounts after death[70] |
| Reddit | Secondary | How do I delete my account?[39] |

Table 6.2: Overview of digital service providers' policies regarding deceased user accounts

Out of the twenty service providers examined, 14 offer official documentation addressing post-mortem account management, such as deactivation, deletion, or access transfer. This high proportion indicates a growing awareness among major digital platforms of the importance of clear post-mortem policies. However, for six of the service providers, as seen in Figure 6.2, only secondary resources or indirect references to post-mortem management could be identified. In these cases, information was often limited to help pages about account inactivity or general deletion procedures, rather than dedicated guidance for handling accounts of deceased users. Notably, even among providers with official resources, the accessibility and clarity of these policies varied considerably. Some documents were challenging to locate, interpret, or navigate, which may pose barriers for grieving families or estate executors seeking assistance. Although a high number of platforms now provide official policies on post-mortem account management, the presence of these policies is not sufficient if they are difficult to access or understand.

The following two parts of the analysis examines the specific procedures required by each platform in order to assess their practical usability. The first part examines inactivity-based deactivation procedures, focusing on what happens to the account of the user, if no action is taken after the users death, and explores the policies and time frames for account deactivation or deletion due to inactivity. The second part of the analysis addresses procedures that can be initiated by users and NOK, exploring the options for users to prepare their accounts in advance, as well as the actions that NOK can take, both when the user has taken prior action and when no such preparations exist.

6.2 Passive deactivation procedures

An important aspect is how service providers handle account inactivity and whether they suspend or delete accounts that remain unused for a certain period. As shown in Figure 6.1, most providers do not apply automatic suspension or deletion based on inactivity. 14 out of 20 platforms take no action when an account is inactive, while six have set time frames for inactivity before suspension or deletion occurs. Three providers act after 24 months of inactivity, and three providers uses a threshold of 1, 4, or 12 month. This variation shows that, for most platforms, inactive accounts remain accessible unless a user or their family takes specific action. Only a minority of providers have clear policies with defined periods of inactivity leading to suspension or deletion. This indicates that handling of accounts after the death of a user has to involve explicit post-mortem procedures, rather than rely solely on inactivity-based measures.

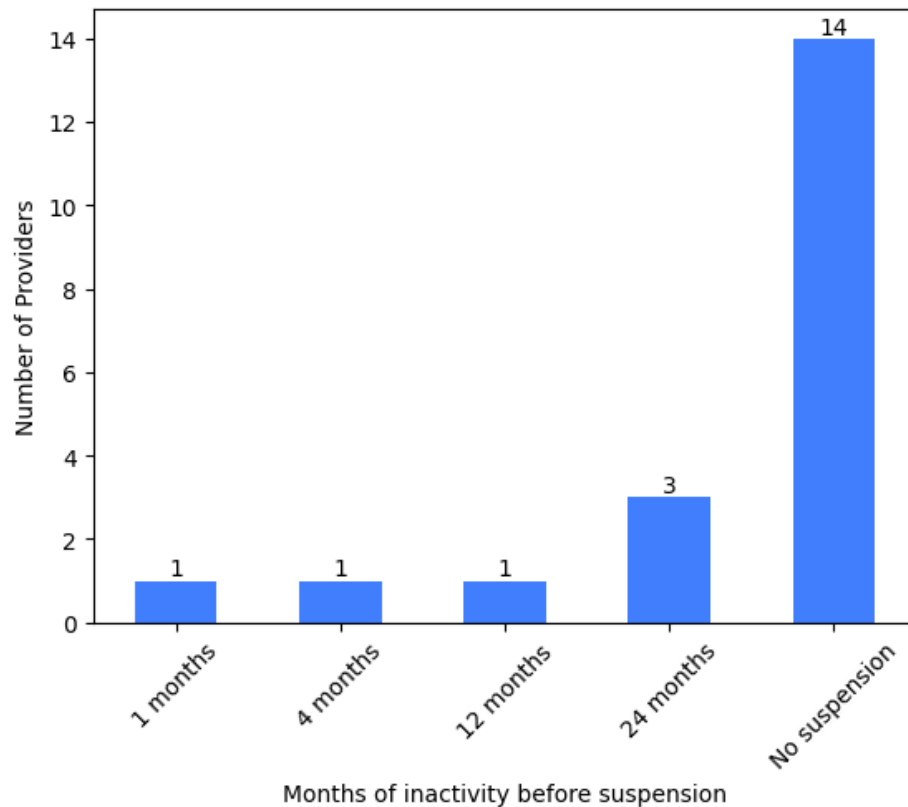


Figure 6.1: Distribution of service providers by inactivity suspension policy, showing the number of platforms that apply account suspension or deletion after specific periods of inactivity.

Some providers include additional notes or exceptions in their inactivity policies:

- **Google:** The policy applies only to personal accounts with no affect on business accounts. Google reserves the right to delete a personal account and its contents after 2 years of inactivity. Before deletion, Google sends multiple notifications to both the account and recovery email addresses. Activities such as signing in, using any Google service, or maintaining a subscription are sufficient to keep the account active.[77]
- **WhatsApp:** Accounts are deleted after 120 days of inactivity to limit data retention and protect user privacy. The content stored locally on the device of the user will be available until the application is deleted, but the account itself is permanently deleted.[1]
- **X (Twitter):** Users must log in at least every 30 days to keep their accounts active. X has indicated plans to archive or remove accounts left inactive for "*several years*", but the current inactive account policy still requires regular logins to avoid possible

deletion.[9]

In Figure 6.2, an overview of the service provider analysis is presented. The table columns indicate whether the provider has a dedicated policy for post-mortem data management, the availability of account deactivation or deletion after death, the presence of memorialisation features, inactivity-based suspension options, and the level of access granted to NOK, both with and without prior user action in terms of post-mortem preferences. Additionally, the table specifies the type of heir model each provider uses.

| | Type | Policy | Deactivation / Deletion | Memorialization | Inactivity suspension | Default access* | Transfer of access** | Heir type |
|-------------------|------------------|--------|-------------------------|-----------------|-----------------------|-----------------|----------------------|-------------------|
| Google Account | Account Service | Yes | Yes | Yes | 24 mo | Limited access | Full access | Legacy Contact |
| Microsoft Outlook | Account Service | Yes | Yes | No | 24 mo | No access | Full access | Legacy Contact |
| Apple Account | Account Service | Yes | Yes | No | 12 mo | Limited access | No access | Legacy Contact |
| Whatsapp | Communication | No | Yes | No | 4 mo | No access | No access | Not available |
| Signal | Communication | No | No | No | N/A | No access | No access | Not available |
| Discord | Communication | Yes | Yes | No | 24 mo | No access | No access | Not available |
| Coinbase | Crypto Exchange | Yes | Yes | No | N/A | Limited access | Limited access | Not available |
| Netflix | Entertainment | Yes | Yes | No | N/A | No access | Full access | Not available |
| Steam | Gaming | No | Yes | No | N/A | No access | No access | Not available |
| 1Password | Password Manager | Yes | No | No | N/A | Full access | Full access | Password Handover |
| NordPass | Password Manager | Yes | No | No | N/A | Limited access | No access | Legacy Contact |
| Bitwarden | Password Manager | Yes | Yes | No | N/A | Complicated | Complicated | Legacy Contact |
| SecureSafe | Password Manager | Yes | Yes | No | N/A | No access | Full access | Legacy Contact |
| Snapchat | Social Media | No | Yes | No | N/A | No access | No access | Not available |
| Facebook | Social Media | Yes | Yes | Yes | N/A | Limited access | Limited access | Legacy Contact |
| X (Twitter) | Social Media | Yes | Yes | No | 1 mo | No access | No access | Not available |
| LinkedIn | Social Media | Yes | Yes | Yes | N/A | No access | No access | Not available |
| Instagram | Social Media | Yes | Yes | Yes | N/A | No access | No access | Not available |
| TikTok | Social Media | No | Yes | No | N/A | No access | No access | Not available |
| Reddit | Social Media | No | Yes | No | N/A | No access | No access | Not available |

Figure 6.2: Overview of digital service providers' policies and procedures for account deactivation, memorialisation, inactivity suspension, and access transfer to NOK, comparing default and maximum access levels for NOK across major platforms.

*Default access: Level of access granted to NOK if no prior legacy settings were configured.

**Transfer of access: Highest reachable level of access granted to NOK when legacy settings have been configured in advance.

6.3 Reactive user and post-mortem procedures

The next section of the analysis examines whether each provider supports account access, deactivation, deletion, or access to data, detailing the processes involved when a user has made preparations before their death compared to when no preparations exist.

Service providers handle post-mortem account management in several distinct ways. The processes have been categorised into four main approaches:

- **Legacy contact, pre-assigned NOK or emergency access:** The user designates a trusted contact, heir, or emergency access delegate, who according to the policy of the provider, can manage, access, delete, or memorialise the account and its data after death. This procedure is typically established in advance and grants full or limited permissions depending on the policy.
- **Next of kin (NOK) and legal requests:** The NOK or a legal representative can request access to account data, account closure, or deletion by providing required documentation (e.g., death certificate, proof of authority).
- **Inactivity-based suspension:** The service provider automatically restricts access, deactivates, or deletes accounts after a set period of inactivity. *This approach is covered in the previous section about passive deactivation procedures in section 6.2.*
- **No supported process:** The provider does not offer a formal or public process for post-mortem access, deactivation or deletion.

It should be emphasised that while *legacy contact or pre-assigned heir* and *emergency access or estate planning tools* serve similar purposes, this analysis distinguishes between them as follows: *Legacy Contact or pre-assigned heir* refers to controlled, often limited, post-mortem access to the accounts of a user, typically allowing a designated person to manage or memorialise an account after death. In contrast, *emergency access or estate planning tools* is designed to grant a trusted contact full or partial access to sensitive data, such as passwords, in emergency situations, which may include, but are not limited to, the death of the user.

In the analysis, Facebook, Instagram, and WhatsApp are treated as separate service providers, as they handle post-mortem management differently, despite all being owned by Meta[54].

6.3.1 Legacy contact, pre-assigned heir or emergency access

Google Inactive Account Manager

Google allows users to designate up to 10 individuals as legacy contacts, granting them full access to the content of the account. This setup must be completed before the account owner passes away. Access is provided to services such as YouTube, Google Drive, Google Mail, and Blogger. In the absence of any previous action, immediate family members have

the possibility to collaborate with Google to deactivate the account, and under specific conditions, the ability to retrieve content from the account of the deceased.[77] However, without prior arrangements, they will not be able to fully access the account.

Apple Accounts

For Apple Accounts a user designates a legacy contact, who can then use an access key and a death certificate to request access. In cases where the user has not assigned a legacy contact before their death, the NOK is required to present a court order that confirms their entitlement to access or delete the deceased account of the deceased, verify their identity, and seek assistance from Apple.[42]

Facebook

For Facebook a user designates a legacy contact, who then gets the ability to do specific actions on the account following the death of the user. This includes actions such as memorialising the profile, obtaining a copy of shared content, pinning posts, managing friend requests, and changing the profile or cover photo. Additionally, the legacy contact has the authority to request deletion of the account. In instances where no legacy contact has been established, NOK may seek access by providing one document that serves as proof of authority, either a *power of attorney*, a *birth certificate* if the deceased was a minor, a *last will and testament*, or an *estate letter* alongside one document that verifies the death, such as an *obituary* or *memorial card*. [12]

Password Managers

Bitwarden, SecureSafe, and NordPass all offer emergency access or inheritance features that allow users to select trusted contacts who can access their accounts in case of death or emergency. In Bitwarden, users can set up emergency contacts who are granted specific privileges, such as viewing, taking over, or deleting the vault, based on the permissions set by the account owner.[23] SecureSafe enables users to establish account inheritance, allowing a preassigned contact to gain full access to passwords and data after a waiting period and with an activation code.[12] Similarly, NordPass allows users to assign an emergency contact who can request access to their passwords. If the request is not cancelled by the account owner within seven days, access is automatically granted.[59]

1Password is excluded from this category because their post-mortem process is manual and could apply to any service provider. An explanation will follow in subsection 6.3.3, which discusses service providers without a support process.

6.3.2 Next of kin or legal request

Microsoft

Microsoft applies a strict policy on Outlook and Microsoft accounts for deceased users. Generally NOK cannot access the contents of the account, such as emails or files, unless they have the login credentials, or obtain a court order proving right to request access to release the data. Without credentials, family members can request account closure by providing legal documentation, but Microsoft will not share any account contents. Microsoft does not offer legacy planning features for users to plan what happens with their data after death.[3]

Discord

Discord only allows NOK to request the deletion of an account of a deceased user. The NOK must provide detailed information, including the account details, which is the email address and username associated with the account. In addition, they must submit proof of the death of the user, such as a death certificate or coroner's report, as well as documentation establishing their relationship to the deceased, which could be a *marriage license*, *birth certificate*, *last will and testament*, *estate letter*, or *power of attorney*. Finally, the requester must verify their own identity with a valid photo ID or passport. Discord will only process the request for deletion after all requirements, stated above are met.[16]

Coinbase

For Coinbase a user can create a will for their account and specify wallet addresses for receiving funds. Although Coinbase does not offer a legacy contact feature, users can still arrange for their holdings to be transferred to a predetermined wallet upon their death. When the user passes away, the NOK or estate representative must provide certain legal documents to Coinbase in order to request the transfer of assets. The required documents include the following:

- Death certificate
- Probate papers
- Letters Testamentary or Letters of Administration
- Affidavit for Collection or Small Estate Affidavit
- Government-issued ID

Additionally, the estate representative must submit a signed letter instructing Coinbase to transfer all assets to the specified account or wallet, including its associated email address. Once the transfer is complete, the original account can be closed or deleted.

If the deceased did not plan ahead, NOK or representatives are still required to provide all necessary legal documents, and if there is no will or estate plan. The involvement of a probate court may be necessary to determine the rightful representative.[7]

Netflix

In the case of Netflix, the provider allows NOK to cancel an account on behalf of a deceased person. Netflix instruct NOK based on whether they have access to the account or not. If the NOK can log in, they can simply cancel the subscription through the account page. If they do not have access, they should contact Netflix Customer Service and provide information such as the email address or phone number associated with the account, and in some cases, billing details or the death certificate may also be required to verify the request. Once the necessary information is provided and verified, Netflix will process the cancellation to ensure no further billing occurs.[40]

Steam

By default, the company behind Steam, Valve Corporation, makes Steam accounts non-transferable, meaning they cannot be inherited or passed on to others, even through a will. In the event of the death of a user, NOK are generally unable to access or assume ownership of the account, as Steam Support will not facilitate account transfers or provide login credentials, regardless of documentation or estate requests.

For account deletion or closure, NOK must submit comprehensive proof of ownership, such as previous payment information. While some users choose to share account credentials with trusted individuals, this practice violates Steam's Terms of Service and is not officially supported.[64]

Reddit

Reddit only allows NOK to request the deletion of a an account of a deceased user by submitting a request along with basic proof, such as the username, a death certificate, and evidence of their relationship to the deceased.[39]

TikTok

To request deletion of a deceased user's TikTok account, NOK must contact TikTok and provide the full name of the user, email address, a link to their account, a copy of government-issued ID, and a death certificate.[41]

X (Twitter)

For X (formerly known as Twitter), NOK can request the removal of the account of a deceased user by contacting X and providing the following documentation. This process requires the NOK to submit their own government-issued ID, the full name of the deceased, and a copy of the death certificate. Once these documents are reviewed and verified, X will proceed with the removal of the account. It is important to note that X does not offer options for accessing the account, transferring its contents, or memorialising it. For post-mortem management, account removal is the only available action.[9]

LinkedIn

LinkedIn offers both memorialisation and account deletion for deceased users. If a person are authorised to act on behalf of the deceased, such as NOK or estate representative, they can request to close the account by submitting the following information:

- Full name of the user
- Profile URL
- Account email
- Date of death
- Link to an obituary or news article
- Death certificate
- Relationship of the requester to the deceased
- Legal proof of authority, e.g. *Letters of Administration* or *Testamentary*

If a person is not authorised, they can still report the death, and LinkedIn will memorialise the profile by locking access and displaying a memorial badge to preserve the person's legacy. However, it was not possible during the analysis to determine the specific basis on which account closure requests are approved. Additionally, there is a potential risk of false reports for memorialising an account, as the requirements are less strict than those for closing an account. In both cases, LinkedIn does not provide access to the account or disclose login credentials to anyone.[10]

Instagram

Instagram allows NOK to request deletion or memorialisation of the account of a deceased user. To proceed with either options, the requester must provide documentation such as the birth certificate and death certificate of the deceased, as well as proof of their relationship to the deceased or legal proof of authority to act on their behalf. Memorialisation

keeps the content of the user visible as a tribute, while deletion removes the account and all associated data from the platform.[67]

6.3.3 No support process

As illustrated in the overview in Figure 6.2, most of the service providers included in the analysis offer some form of account deactivation or deletion. In particular, WhatsApp, Snapchat, Signal and 1Password do not provide any mechanism for account closure after the death of a user.

WhatsApp

If an individual have the login information for a WhatsApp account, it can be manually deleted directly from the app on the device of the deceased. Without access to the device, you may try contacting WhatsApp support and provide information about the deceased, but there is no formal process or dedicated policy in place for handling such requests. Importantly, WhatsApp automatically deletes accounts after 120 days of inactivity to limit data retention and protect privacy. This means that if no one logs in or uses the account during that period, it will be removed without further action required.[1]

Snapchat

Snapchat does not have an official post-mortem policy or memorialisation option for the deceased users. While some sources, such as Simplicity, suggest that account deletion is possible if the NOK submits a death certificate, this process is not clearly defined or officially documented by Snapchat itself.[70]

Furthermore, the information about submitting a death certificate remains unverified by Snapchat and is based on third-party guidance rather than an explicit policy.[43]

Signal

The policy of Signal is centred on privacy and security. Accounts are registered to a phone number and managed solely by the user on their device, with no access to messages or account content by Signal or third parties. Signal does not provide a process for others to close or manage an account on behalf of the NOK, including in the event of death. All account data and messages are stored only on the device of the user, and account deletion can only be performed from within the app on that device. If a phone number is deactivated and reassigned, the previous Signal account linked to that number is automatically deactivated.[17]

1Password

1Password does not provide a formal legacy or post-mortem access process for individual accounts. Access after death is only possible if a trusted party has the master password and Secret Key. 1Password recommends using their *Emergency Kit* which is a PDF document. However, sharing passwords as a solution for post-mortem data management is not recommended or accepted in this analysis, as it undermines privacy, increases legal and security risks, and can expose sensitive data to unauthorised parties, potentially violating both the deceased and third parties privacy.[83]

Based on the policies of both Signal and 1Password, user accounts will persist indefinitely following the death of a user, as none of the providers has a clear policy or mechanism for account suspension or deletion due to a NOK taking action or inactivity. This means that these accounts remain active and could pose a risk in the case of leaked account credentials.

6.4 Service provider risk assessment

There is significant variation in how service providers handle account post-mortem scenarios. Therefore, not all providers should be expected to follow the same standards, as they hold different types of data and, in the case of email or account providers, may grant access to other services. Therefore, it is important to have a method for quantifying the extent to which a service provider should manage, handle, and protect the data and accounts of deceased users. In line with best practices in cybersecurity, this analysis applies a risk assessment to each platform to determine the relative importance of the provider.[81] This approach enables a clearer understanding of the potential impact if a provider does not take sufficient measures to protect accounts.

The risk analysis conducted is based on severity levels. The severity levels defined in Table 6.3 takes inspiration from an industry standard named Common Vulnerability Scoring System (CVSS)[44] and is a widely recognised incident severity models. This model categorise risk and impact into *Critical*, *High*, *Medium*, and *Low* levels based on potential harm, data sensitivity, and possible consequences.

| Severity level | Industry standard description | Contextualised description |
|----------------|---|---|
| Critical | Catastrophic harm, total loss, major data exposure | Compromise would severely impact the estate or privacy of the deceased, exposing highly sensitive data or enabling access to other linked accounts and services |
| High | Significant sensitive data, major financial/legal/reputational harm | Compromise could grant access to important personal or financial data of the deceased, causing significant legal, financial, or reputational harm. |
| Medium | Moderate data, inconvenience, impersonation, moderate harm | Compromise may expose moderate personal or social information, leading to inconvenience or distress for relatives, but not severe or lasting harm |
| Low | Minimal data, limited impact | Compromise would affect non-sensitive accounts, resulting in minimal practical or emotional consequences for survivors |

Table 6.3: Mapping of industry standard severity levels to contextualised risk analysis levels

The following table categorises the service providers analysed according to severity levels. This classification is based on the types of data the providers hold and the potential consequences of misuse or unauthorised access to the accounts they host. The mapping, presented in Table 6.4, expands upon the initial grouping shown in Table 6.1 at the beginning of the service provider analysis.

| Category | Service Providers | Severity Level | Rationale |
|-------------------|--|----------------|---|
| Password Managers | Bitwarden SecureSafe NordPass 1Password | Critical | Compromise exposes all stored credentials, enabling access to a wide range of other accounts and sensitive assets. |
| Mail Provider | Microsoft Outlook | Critical | Central for identity and password resets. Compromise enables access to other accounts and sensitive communications. |
| Account Services | Google Account Apple Account | Critical | Provides access to multiple linked services and devices. Compromise can broadly affect digital identity and assets. |
| Crypto Exchange | Coinbase | High | Direct financial assets are at risk. Compromise can result in irreversible financial loss. |
| Communication | Signal WhatsApp Discord | High | Contains sensitive conversations and contacts. Breach can expose private communications and social circles. |
| Social Media | Facebook X (Twitter) LinkedIn Instagram TikTok Snapchat Reddit | High | Contains extensive personal data and social connections. Compromise can lead to impersonation, fraud, or reputational harm. |
| Gaming | Steam | Medium | Stores payment info and digital assets. Breach may result in financial loss or impersonation, but impact is typically limited to gaming assets and inventories. |
| Entertainment | Netflix | Low | Mostly personal preferences and some payment info. Compromise has minimal direct impact. |

Table 6.4: Severity levels, service providers, and rationale for each category relevant to post-mortem digital account management.

The analysis presents password managers and email providers as *Critical* due to their central role in digital identity and access to other accounts. In contrast, entertainment services are considered *Low* risk given their limited data sensitivity and impact.

Overall, this approach ensures that post-mortem digital account management is guided by a clear understanding of risk, enabling more effective decision-making and resource allocation to safeguard sensitive data and digital assets.

6.5 Overview of findings and insights

The analysis reveals significant differences in how service providers approach post-mortem account management, both in terms of policy availability and practical implementation.

Several themes and gaps emerged across providers, highlighting challenges for users, families, and estate representatives navigating digital legacy issues.

- There is substantial variation in how service providers handle post-mortem account management, both in terms of policy availability and practical implementation.
- Out of 20 providers, 14 offer some form of official post-mortem documentation, but the clarity, accessibility, and detail of these policies differ widely.
- Six platforms lack dedicated post-mortem procedures, relying instead on indirect or incomplete guidance.
- Inactivity-based deletion or suspension is only available in six out of 20 platforms, so most accounts will persist unless explicit action is taken by users or NOK.
- Legacy contact, pre-assigned heir, or emergency access features are only available on seven platforms: Google, Apple, Microsoft, Facebook, and the password managers NordPass, Bitwarden, and SecureSafe.
- Access for NOK through legal requests for account access or deletion are common, but high and varying documentation requirements, making the process burdensome and inconsistent, particularly during the grieving period.
- 50% of providers block access regardless of user or legal action, while the other 50% allow access if steps were taken before death or through legal means.
- Memorialisation options are inconsistently implemented, even among platforms owned by the same company (e.g. Facebook, Instagram and WhatsApp).

Chapter 7

Analysis of Survey and Interviews

7.1 Quantitative survey results

The survey aimed to explore general awareness of digital legacy, personal experiences with post-mortem data management, and the steps individuals in Denmark have taken to plan their digital afterlife. It also examined attitudes toward data ownership, digital guardianship, and the handling of cryptocurrency assets, as outlined in the questionnaire in section 4.3.

To ensure a broad reach, the survey was distributed via LinkedIn and Facebook and remained open from 20 February to 25 March 2025. During this period, 140 individuals completed the questionnaire. A complete set of quantitative survey data can be found in Appendix C.

| Demographic | Count | Percentage |
|--|-------|------------|
| Age | | |
| Below 30 years | 77 | 55.0% |
| 30-49 years | 31 | 22.1% |
| 50-69 years | 29 | 20.7% |
| +70 years | 3 | 2.1% |
| Occupation | | |
| Full-time employed | 64 | 45.7% |
| Student | 47 | 33.6% |
| Self-employed | 12 | 8.6% |
| Unemployed | 8 | 5.7% |
| Other | 9 | 6.4% |
| Digital dependency | | |
| Uses digital solutions for almost everything | 81 | 57.9% |
| Uses them daily but could do without some | 52 | 37.1% |
| Uses only when necessary | 7 | 5.0% |
| Actively uses social media | | |
| Yes | 124 | 88.6% |
| No | 16 | 11.4% |
| Knows the term "digital legacy" | | |
| Yes | 20 | 14.3% |
| No | 120 | 85.7% |

Table 7.1: Demographic breakdown of survey respondents. The total number of respondents is $n = 140$.

The demographics of the respondents are shown in Table 7.1. Most respondents are under the age of 30 (55%), with approximately 20% in both the *30-49 years* and *50-60 years* age groups. Full-time employees make up 45.7%, followed by students at 33.6%. A majority (57.9%) report a high digital dependence, supported by 88.6% using social media actively. To establish a baseline, respondents were asked about the term "*digital legacy*" and 85.7% did not know it. Respondents who answered "*no*" were given a brief intro to digital legacy for clarity.

The respondents is primarily composed of younger and highly digitally engaged individuals, which may introduce bias and limit the generalisability of the findings.

Table 7.2 shows that 131 of the respondents (93.6%) has never handled the digital legacy of a deceased person. The low number of respondents who have handled a digital legacy may be affected by the younger demographic, which has limited exposure to death events, or a potential lack of awareness of what constitutes digital legacy handling. However, the scope of this survey does not provide insight into the reasons behind this distribution.

| Handled deceased person's digital legacy | Count | Percentage (%) |
|--|-------|----------------|
| Have not handled | 131 | 93.6% |
| Have handled | 9 | 6.4% |

Table 7.2: Distribution of respondents who have handled a deceased person's digital legacy. The total number of respondents is $n = 140$.

Table 7.3 displays the distribution of respondents in whether they have handled their own digital legacy or not.

| Handled own digital legacy | Count | Percentage (%) |
|----------------------------|-------|----------------|
| Have not handled | 130 | 92.8% |
| Have handled | 10 | 7.2% |

Table 7.3: Distribution of respondents who have handled their own digital legacy. The total number of respondents is $n = 140$.

Figure 7.1 compares whether respondents took any action for their own digital legacy, based on whether they have handled the legacy of a deceased person or not. Among those who have handled a digital legacy, 11.1% have taken action on their own, compared to 6.9% of those who have not.

Although the difference is small, the data may suggest that a firsthand experience could play a role in prompting action.

However, based on the difference, it is not possible to determine what factors prevents respondents from taking action. Even though Figure 7.1 does not directly capture deeper motivations or barriers, an overview of the reasons for lack of action is presented in Figure 7.6.

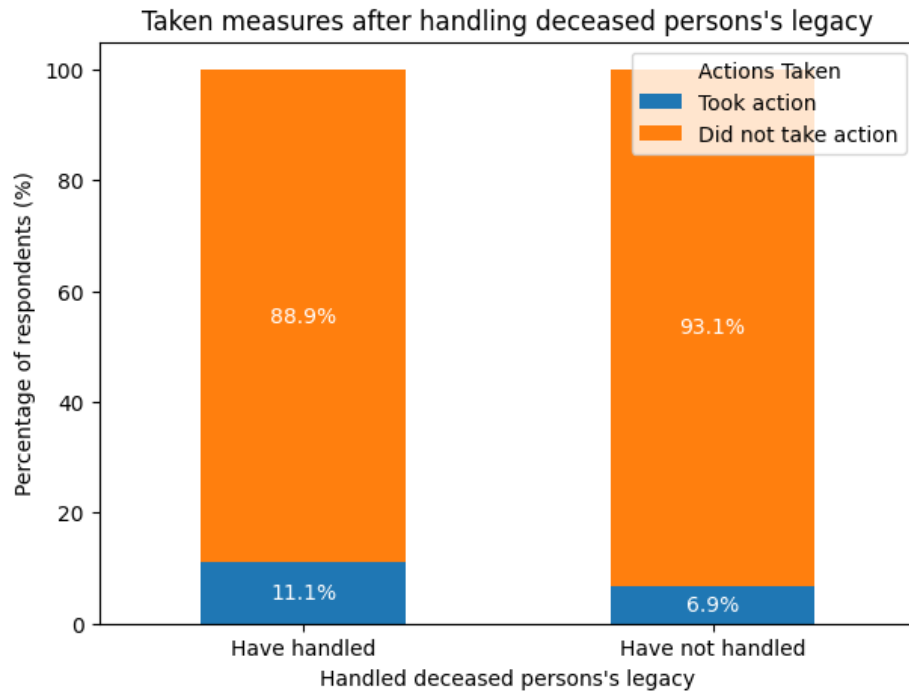


Figure 7.1: Distribution of respondents who took action on their own digital legacy. 11.1% did so after handling a digital legacy, compared to 6.9% without prior experience

While an experience may have some effect, awareness appears to be more impactful. Figure 7.2 shows how knowing about digital legacy relates to taking action. The basis for *knowing* is whether respondents answered “yes” to knowing about the term “digital legacy”.

Respondents who knew about digital legacy were more likely to act, with 20% taking action compared to 5% among those unaware. Despite the increase, 80% of those aware of digital legacy had still not taken action. This suggests awareness helps but does not explain most behaviour.

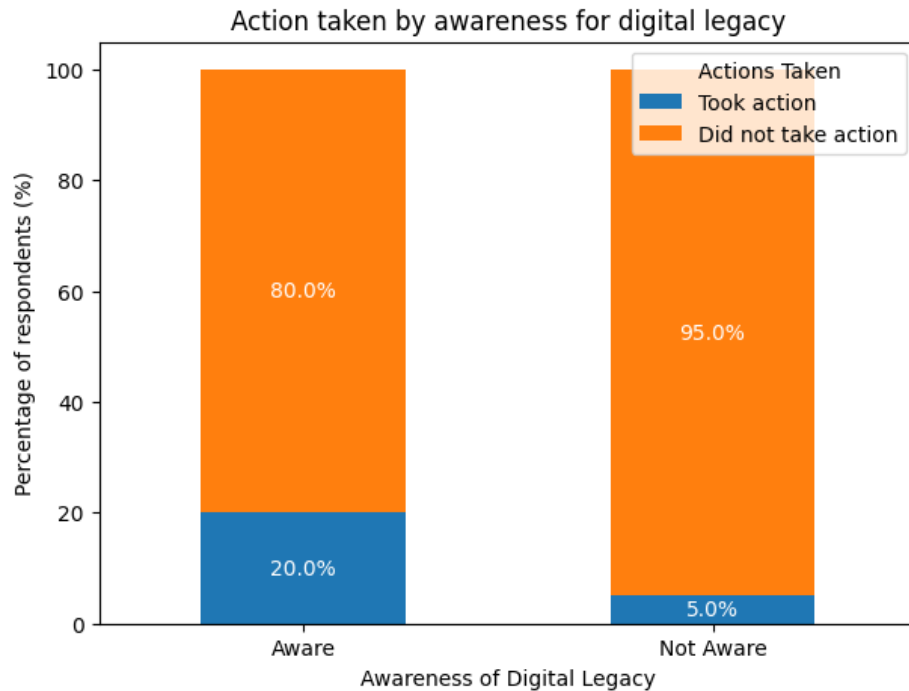


Figure 7.2: Distribution of respondents by awareness and action. 20% of those aware had taken action, compared to 5% of those unaware.

Beyond awareness and experience, the specific platforms the user is active on may also influence behaviour. Figure 7.3 presents whether using more intimate platforms like Snapchat or Instagram relates to if respondents have taken action.

Snapchat and Instagram was selected based on a study by Kofoed and Larsen in 2016[51], that explored photo-sharing practices among young people, which suggested that Snapchat and Instagram is often used for sharing unfiltered, spontaneous images, which support the description of the two platforms as *intimate*.

Figure 7.3 shows that respondents who regularly use Snapchat, Instagram, or both are less likely to have taken action. Only 6.3% of users have taken action, compared to 10.3% of non-users. As the difference is small, it cannot be used to conclude whether the use of intimate platforms affects if users take action of their digital legacy.

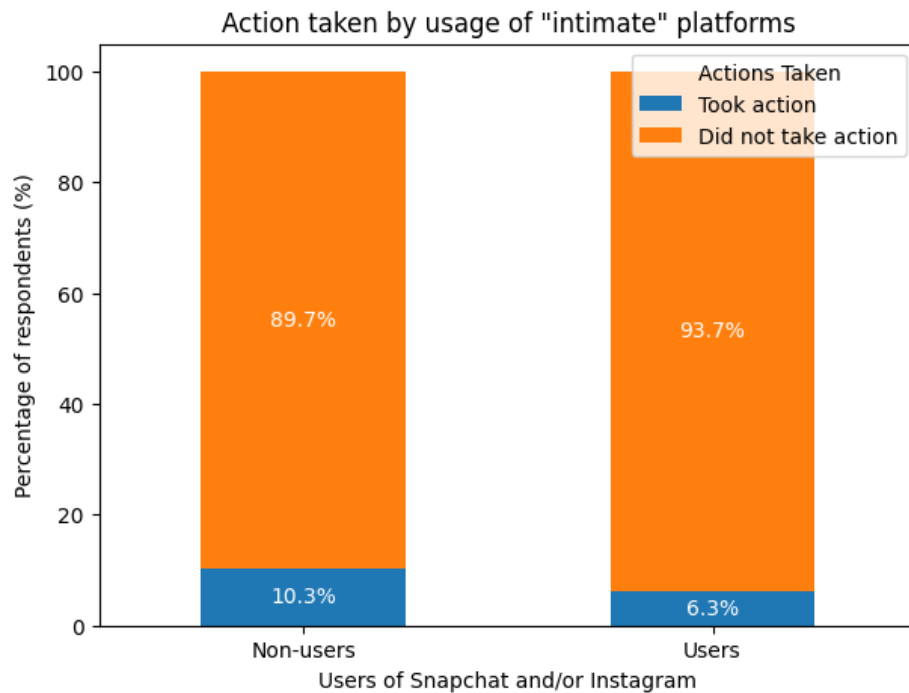


Figure 7.3: Distribution of actions taken for digital legacy among users and non-users of intimate platforms. 6.3% of users have taken action, compared to 10.3% of non-users.

Another factor that may influence whether the respondent have taken any action is their age. Figure 7.4 shows how whether respondents have taken action based on their age group.

The results shown in Figure 7.4 displays that action is low across all age group. The age group with the highest level of action is 30-49 at 12.9%.

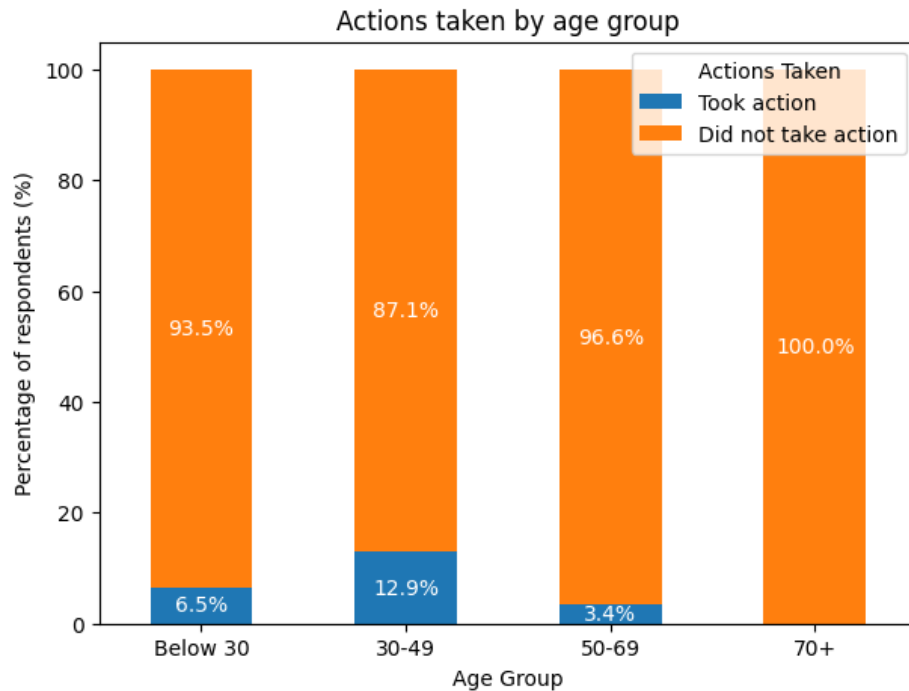


Figure 7.4: Distribution of actions taken for digital legacy across age groups. Few respondents in any group have taken action, with the highest rate at 12.9% among those aged 30-49 and none in the 70+ group.

This increase in action by the 30-49 age group raises the speculative question of whether it is influenced by their position at a cross-section, old enough to consider death or inheritance, yet still digitally proficient.

To explore this, Table 7.4 shows digital proficiency by age. However, the 50-69 group scored higher in *Daily, but not all* use, 41.4% compared to 25.8%, and lower in *Only when necessary* 3.4% vs. 16.1%, contradicting the previous assumption.

| Age group | Only when necessary | Daily, but not all | Almost everything |
|-----------|---------------------|--------------------|-------------------|
| Below 30 | 1.3% | 37.7% | 61.0% |
| 30-49 | 16.1% | 25.8% | 58.1% |
| 50-69 | 3.4% | 41.4% | 55.2% |
| 70+ | 0.0% | 100.0% | 0.0% |

Table 7.4: Self-reported digital dependency by age group.

In addition to age, digital dependency may influence awareness. The next figure explores how the three levels of digital dependency, from Table 7.1, relate to awareness of digital legacy.

Figure 7.5 shows that respondents who are highly digitally dependent, “Almost everything”, are not significantly more aware than those with moderate or low dependency. This suggests that even highly digitally dependent users may not have been exposed to digital legacy planning, and the same appears true for all other levels of digital dependency as well.

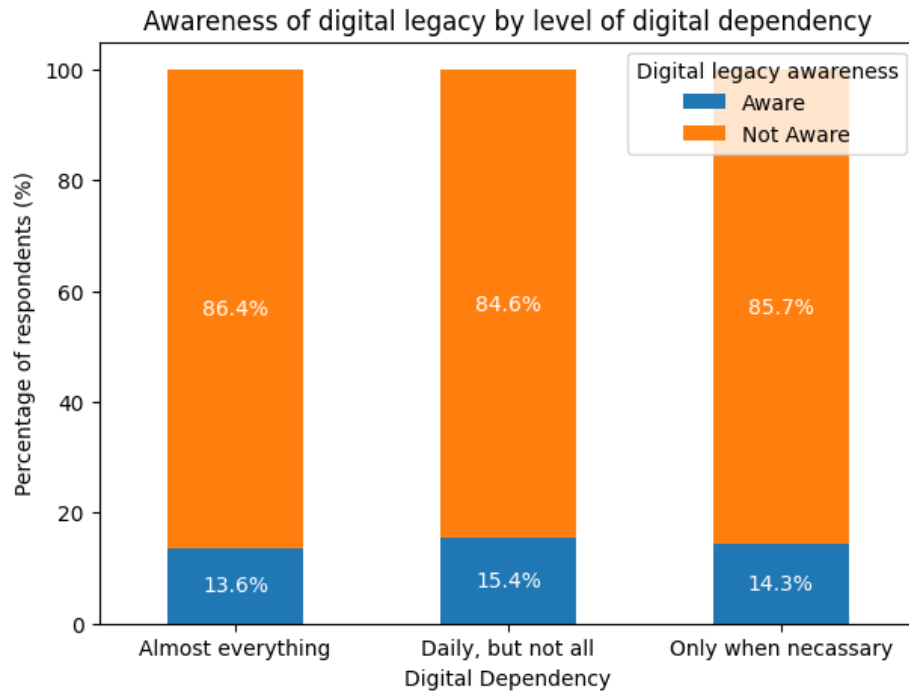


Figure 7.5: Distribution of digital legacy awareness by digital dependency. Awareness is low across all levels, with fewer than 16% of respondents aware in any group.

To understand why most respondents had not taken action, they were asked to select reasons for not handling their digital legacy.

Figure 7.6 shows that the most common reason for not making a digital legacy plan is not having thought about it, chosen by 76 respondents. This is followed by not knowing how to do it, chosen by 41. 8 respondents pointed to the lack of a clear solution. The data suggests that most people have not engaged with digital legacy planning simply because they have not thought about it or do not know how.

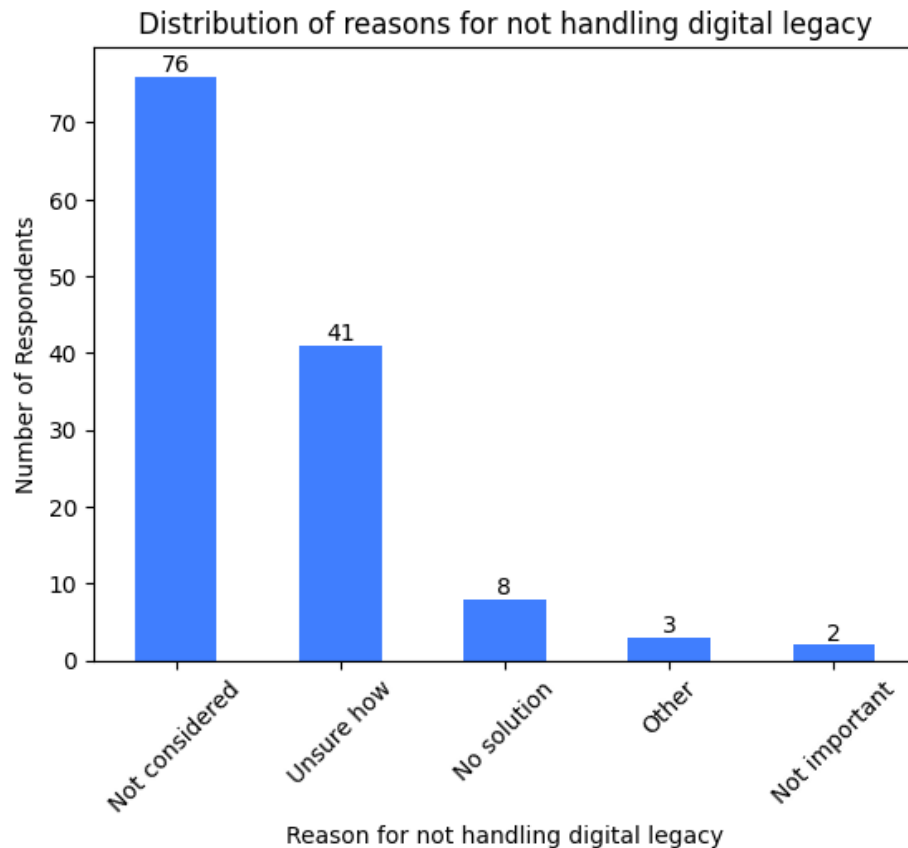


Figure 7.6: Distribution of reasons for not handling digital legacy. Most respondents had simply not considered it (76), followed by uncertainty about how to proceed (41). Few answered lack of solutions, importance, or other reasons.

In contrast, among those who have taken action, the most common steps are manually documenting account access details, such as passwords, informing a trusted person or family member, or using the service providers existing tools, explored in chapter 6, to assign a digital legacy contact.

Examples of actions taken by respondents (*translated from Danish*):

- "I have added a relative as my legacy contact on Meta to ensure others can access my account."
- "I have written down some wishes, initially shared with my partner, who can request access to my password vault."
- "I have filled out a declaration specifying who should have access to my Apple products after my death."

- *"I have set up a family member as my heir."*
- *"I have stored my password vault key and private keys on a USB stick in a box at home, along with a backup YubiKey."*
- *"My daughter has all my codes."*
- *"I have specified who can access my profile if I die (I think this can only be done on Facebook); otherwise, all my codes are written in my will."*
- *"I have given my email and password to a trusted family member, who is also set as my legacy contact on Facebook."*
- *"I have added my sister and husband as legacy contacts through Apple, so they'll get access to my iCloud data in the event of my death."*
- *"I have written my codes down."*

Most actions are simple, such as sharing passwords or writing down instructions, while formal legal planning is rare. Those who take action typically focus on ensuring access for loved ones rather than setting up detailed or legally binding arrangements.

Respondents were asked to decide how they would prefer their digital data to be handled after their death. Six different options were presented, and the distribution of responses is illustrated in Figure 7.7.

The following shows the mapped entry used in Figure 7.7 and its a translated version of the original phrasing in the survey:

- **Delete all:** Delete all my accounts and data permanently.
- **Appoint full-access heir:** Appoint a person with full access to my accounts.
- **Partial data handover, full deletion:** Delete my accounts, but transfer selected data to specific people.
- **Appoint partial-access heir:** Appoint a person with partial access to my accounts.
- **Segmented data sharing:** Categorise my data and grant access based on type and person.
- **Partial deletion with data retention:** Delete some accounts, but retain selected data.

The distribution shows a mix of approaches to how users want their metasoul handled. A clear preference for deletion is popular, at 49 respondents, followed by 33 respondents preferring giving full access to a NOK. 28 respondents preferred deletion of their data, while simultaneously transferring selected data to specific individuals.

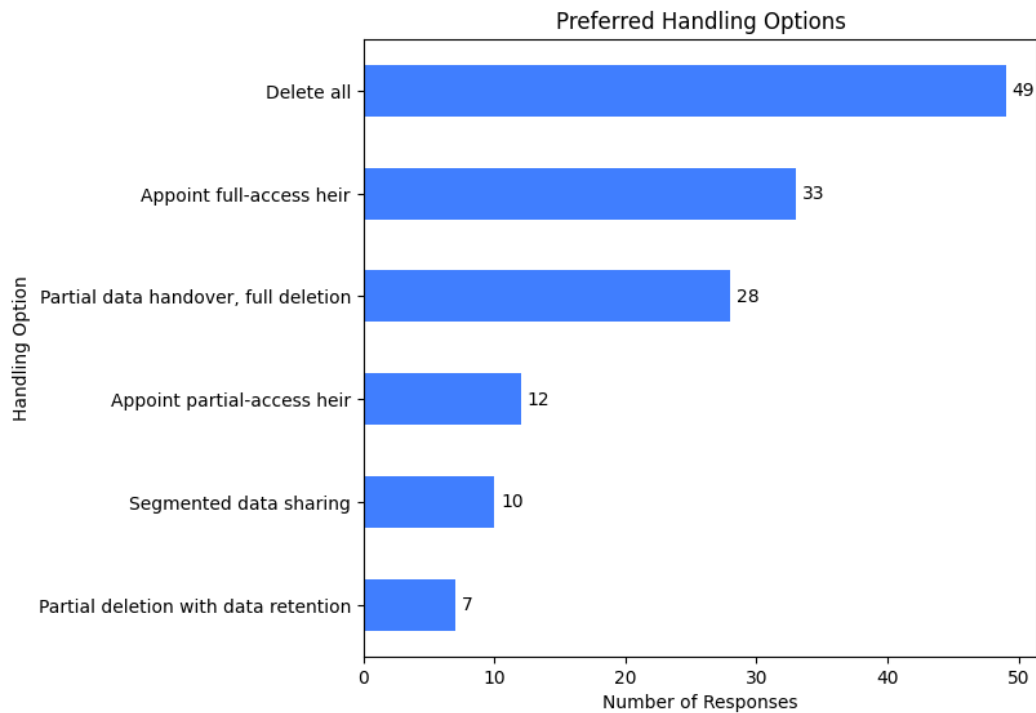


Figure 7.7: Distribution of preferred digital legacy handling. Most prefer full deletion, followed by full-access heirs or full deletion combined with partial handover.

After looking at overall preferences, five platforms were selected, inspired by their popularity among users[6], to see if choices vary depending on the service.

Figure 7.8 shows that deletion is most preferred among users, averaging 64.7% across all five platforms. An average of 17.8% would prefer full or partial data transfer to NOK across all platforms. On average only 4.7% want to keep accounts open without any additional action. Finally, an average of 12.7% of the users are not registered to any of the given platforms.

Figure 7.7 and Figure 7.8 both point in a clear direction that respondents are preferring account deletion.

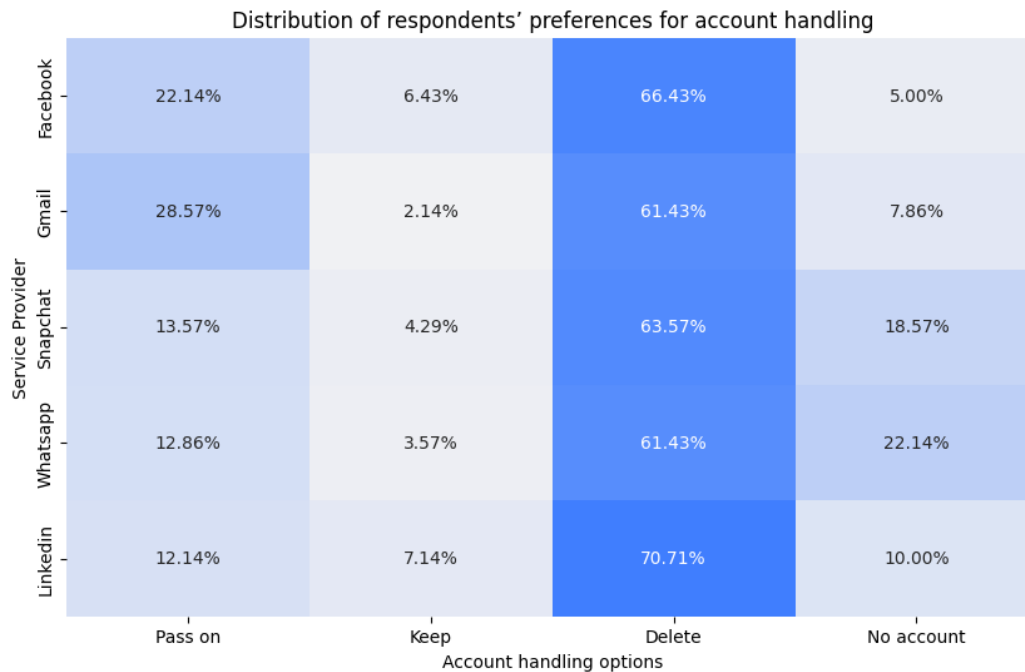


Figure 7.8: Distribution of respondent preferences for actions on different platforms. On average 64.7% prefer to have their accounts deleted.

Regarding holdings of crypto currency, 32 (22.9%) of respondents own cryptocurrency, as shown in Table 7.5. Among those who do, even fewer, at only 8 (25%) have a clear plan for what should happen to their crypto assets after their death. Out of the 32 respondents with crypto currencies, only 9 has shared access with another person. This could indicate that planning for digital assets like cryptocurrency is still rare.

| Crypto-related question | Base (n=) | Yes (%) | No (%) |
|----------------------------------|-----------|------------|-------------|
| Owens cryptocurrency | 140 | 32 (22.9%) | 108 (77.1%) |
| Has made a plan for their crypto | 32 | 8 (25.0%) | 24 (75.0%) |
| Has shared access credentials | 32 | 9 (28.1%) | 23 (71.9%) |

Table 7.5: Overview of respondents' cryptocurrency ownership, planning, and access sharing.

7.2 Qualitative interview results

This section analyses themes that emerged across the collected interviews with stakeholders and individuals who have directly dealt with digital death either in an organisation or personally. The purpose of this analysis is to better understand how post-mortem data is handled in practice, where the current challenges lie, and what kinds of changes or

structures users would like to see implemented.

The analysis is structured by themes based on commonalities across interviews, with one or more interviews included per theme. The full list of interviews is listed in Table 4.2 and questions asked is available in Appendix A.

Immediate system lockout and loss of access

A recurring challenge raised in both organisational and personal contexts was the immediate deactivation of digital services, particularly MitID[57], the digital identity system in Denmark, and e-Boks[22], a secure email provider used by residents in Denmark.

Johan Niordson, IT Lead and surviving spouse, explained how just days after the death of his wife, her digital identity was entirely shut down, leaving him unable to access even joint accounts or view necessary financial documents.

Similarly, in the case of Sakariye Ali, involving the death of his father abroad, the family was unable to deactivate or manage online services. This was a result of Danish legal barriers, that do not accept the death certificate from abroad.

Bilal, Head of IT-support and Janni, CISO, from Syddansk Universitet, later mentioned as SDU, described how email accounts and OneDrive folders are locked as part of a default process upon notification of death. While this serves a security purpose, they reported often creates significant friction for family members or colleagues who need access to files, emails, or documents to wrap up the affairs of the deceased. An emerging issue is that lockout procedures prioritise security over usability, often leaving little or no grace period for retrieving essential information.

Case-by-case handling and lack of standardised protocols

At SDU, the approach to post-mortem data management is largely case-by-case, relying heavily on internal communication between the IT- and HR departments as well as the immediate leader of the deceased person. Currently, SDU is building on top of existing procedures for producing clearly documented, standardised workflows, so that access to data is handled in a unified way.

In one specific case, this lack of procedure extended to external platforms, as a employee used the work mail account for external platforms. However, these accounts was only accessible because the deceased had shared passwords to NOK, which raises ethical and security concerns, for handling such cases. Some of the insights are that the absence of documented, transparent policies makes post-mortem digital access dependent on individual interpretation, privilege, and persistence.

Legal and jurisdictional conflicts across borders

The situation involving the father of Sakariye Ali, who passed away in Somalia, highlights a deeper jurisdictional blind spot. When a person dies abroad, Danish systems may not recognise foreign-issued death certificates, even for Danish citizens. As a result, critical systems like CPR, pensions, or Facebook do not register the person as deceased, effectively keeping their digital identity active despite their passing. The full story is available on the website of *TV2 Nyheder*.^[60]

This limbo created both emotional and logistical strain, as family members continued to receive auto-generated messages from public organisations and were left unable to close or access accounts.

In the interview with the privacy engineer lecturer, from Aalborg University, insights were provided into the practical challenges of implementing post-mortem data management. They emphasised that while the topic is increasingly relevant, it remains legally and technically complex. From their perspective, service providers are often hesitant to act on post-mortem data without clear legal backing, partly due to the risk of violating privacy laws or contractual obligations.

They also pointed out that current systems are rarely designed with digital legacy in mind, which makes it difficult to implement legacy management features in current solutions. Moreover, they noted that user awareness is generally low, which is in alignment with the findings from the quantitative survey in section 7.1. They also mentioned that most people do not actively consider what happens to their data after death. In their view, any solution must be both legally compliant and simple for users and service providers to adopt.

Emotional impact and ethical tensions

Across the interviews, there was a shared sense of emotional friction. Navigating post-mortem access often involved grief, frustration, and a perceived lack of recognition from systems and institutions.

Johan expressed deep irritation that despite having been married and sharing data, he was blocked from access due to the rigid interpretation of digital ownership.

Astrid Waagstein raised the ethical question of who should have the right to view or use data like photos, emails, or social media posts. She stated that systems need to work towards a more “*granular access*” since a lot of systems are “*super rigid*”.

Another point Astrid brought up was the alteration of the persona of a person after death through the generative AI, where based on existing data about the user, new information was generated about them. This could have consequences for the legacy of the person affected, as this could alter living individuals' perception of them. In terms of ethical

takeaway, there is a need for a more sensitive, tiered access model that respects both the privacy of the deceased and the needs of NOK.

Low awareness and lack of planning tools

Most participants indicated that digital death was not something they had proactively planned for. Some expressed regret about not making backups or access arrangements before it was too late. There was also a shared belief that more guidance or education, perhaps through funeral homes, banks, or public digital services, would help people prepare better.

Astrid echoed this, pointing out that the issue is not taken seriously until it is too late. She emphasised the need for design solutions like digital wills and educational campaigns about digital legacy.

Desire for policy reform and infrastructure support

Finally, all participants, whether organisational or personal, agreed that the current system needs legal and infrastructural reform.

Suggestions included, but are not limited to:

- A national platform for handling digital legacy.
- Official legal recognition for digital wills and instructions.
- Centralised overview of digital assets and accounts for an individual.
- Time-limited access rights for next of kin after death.
- Prompting users to plan digital death during *MitID* or *HR* onboarding.

Several interviewees expressed support for laws that would maintain access rights after death if consent had been given beforehand. There was also recognition that digital death should be integrated into broader conversations about estate planning and public digital services.

Chapter 8

Summary of findings

The examination of digital legacy management in this report reveals a number of challenges that includes aspect from the legal review in chapter 5, service provider analysis in chapter 6 and user insights from chapter 7.

Lack of legal requirements and standards

The exploration of legal frameworks revealed a lack of explicit legal requirements that instruct service providers in how they should handle post-mortem data management.

The exploration showed how current practices, in EU, is purely based on the individual Member States implementation of additional regulation on the rights of deceased individuals, extending GDPR. In contrast, it was revealed that China's PIPL, despite studies[48] and statistics[5, 21, 65], showing underperformance in privacy, explicitly covers that the data rights is inherited by NOK upon the death of an individual.

In Denmark, the Danish Data Protection Act extends the GDPR coverage of data rights for 10 years, while Norway and Sweden stays within the current scoping of the GDPR, which excludes deceased individuals.

However the Norwegian Data Protection Authority[13], *Datatilsynet* supplies guiding for how an employer should handle the death of an employee. This entails a recommendation for splitting data in a *PUBLIC/PRIVATE* separation, which allows for better data handling, while still having data privacy in mind. This approach was revealed to be the same during an interview with Syddansk Universitet (SDU), that adapts a similar approach for their employees, despite no Danish ruling on the topic.

The lack of legal regulations is visible in the scattered landscape of how service providers manage digital legacies, as revealed in the analysis of service providers in chapter 6.

Despite the lack of regulations in EU, the exploration revealed the projects of eIDAS 2.0,

offering a cross-border wallet for credential and digital will storage, and ELI, covering digital inheritance, which could be potential stepping stones for future laws or regulations.

Service provider inconsistencies and opaque policies

The analysis of service providers, in chapter 6, revealed significant inconsistency and lack of transparency in their policies for how they manage digital legacies.

Even for the 14 service providers that offered some guidance through policies, the clarity, accessibility and detail differed widely. Inactivity-based deletion was rare, with only 6 providers offering it, leaving 14 providers without any process, leaving accounts to live on after their owners' passing. With only 10 of the 140 respondents having handled their own metasoul, as displayed in Table 7.3, a question arises as to whether these unattended accounts provides an attack service for potential adversaries.

While 7 of the 20 platforms allow for pre-planning, and 3 allowing access or deletion through legal process post-mortem, there is still 10 service providers blocking any access with or without prior action. This inconsistency and varying legal documentation requirements, may leave grieving NOK in a complicated situation when handling the digital legacy of their loved ones.

User unawareness and behaviours

Due to the limitations stated above, many users resort to informal strategies, like sharing passwords with NOK to ensure post-mortem access, as seen in section 7.1. This approach is both insecure and conflicting with recommended privacy and security practices. Furthermore, it places a significant burden on NOK to manage the metasoul of the deceased, based on the findings in section 6.3 and section 7.1.

The user insights that was revealed in chapter 7 underscores a lack of awareness and preparedness among individuals regarding digital legacy planning. 92.8% of users have made no arrangements for what should happen to their metasoul after death. This lack of awareness is also reflected in respondent behaviour, as 76 out of 140 had never considered the topic and 41 were unsure of what to do.

Chapter 9

Proposed solution

Building on the findings in chapter 8, based on the exploration of legal frameworks, analysis of service providers, and user experiences, this chapter introduces the Unified Post-Mortem Access Protocol (UPAP). UPAP is designed as a protocol to enable a standardised way of handling digital legacy management for service providers. The chapter begins by summarising the findings, mentioned in chapter 8 and throughout the thesis, and mapping them gaps to protocol requirements.

The protocol is presented as core principles, along with proposal for how service providers handle the metasoul. The technical aspects of UPAP includes additions to user creation flows, selection of post-mortem preferences, and an improved mechanism for verifying death events.

Finally, the chapter outlines how service providers can implement UPAP and suggests metrics for validation and testing, though no testing was performed.

9.1 Problem definition and scope

Identified gaps and challenges

The design of UPAP is based on the findings presented in chapter 8, in addition to supplementary findings that also shape the design. The following list outlines the additional gaps that were found:

- **No granular asset selection:** Platforms typically lack support for partial inheritance preferences, offering only binary options such as full deletion or retention of accounts (section 6.3, chapter 8).
- **No standard death verification, inconsistent triggers:** Death verification procedures

vary widely between platforms, with no consistent process for confirming or initiating post-mortem handling (section 6.3, section 7.2, chapter 8).

- **Inconsistent handling format:** Without a shared standard across platforms, post-mortem data management formats and procedures are highly inconsistent, leading to confusion for next of kin (chapter 6, chapter 8).

9.1.1 Scope of service providers

Based on the risk categorisation and findings, presented in section 6.4, UPAP is designed to support service providers that handle sensitive digital assets and represent significant risk in the event of post-mortem account compromise.

The following categories are prioritised due to their *high* or *critical* severity levels:

| Category | Severity | Description |
|---|----------|---|
| Password Managers (e.g., Bitwarden, 1Password) | Critical | These services store login credentials and provide access to a wide range of accounts and sensitive data. |
| Mail Providers (e.g., Microsoft Outlook) | Critical | Email accounts are central to digital identity and are often used for password resets, making them a critical access point. |
| Account Services (e.g., Google Account, Apple Account) | Critical | These providers manage access to multiple linked services and digital content. |
| Crypto Exchanges (e.g., Coinbase) | High | Platforms with access to financial assets, where breaches can lead to irreversible monetary loss. |
| Communication Platforms (e.g., Signal, WhatsApp, Discord) | High | Contain sensitive conversations and contact data that require privacy even post-mortem. |
| Social Media Platforms (e.g., Facebook, Instagram, LinkedIn, TikTok) | High | Host extensive personal data, photos, and social connections. Compromise can lead to impersonation or reputational harm. |

Table 9.1: Categories of digital services and their post-mortem relevance

9.2 Requirements specifications

This section defines the functional and non-functional requirements for UPAP, presented in Table 9.2 and Table 9.3. The requirements are mapped, prioritised using MoSCoW[66], and based on the findings in chapter 8 and the gaps described previously in section 9.1.

Functional requirements

| Priority | Requirement |
|-------------|--|
| Must have | The ability to verify death event requests with high confidence, without requiring changes to the existing death certificate verification processes of the service provider. |
| Must have | The ability to verify death events without relying on third-party organisations or country-specific authorities for death certificate validation. |
| Must have | A standardised process across service providers for authenticating the NOK in the event of a death request. |
| Must have | The ability to notify relevant parties and logging of all actions regarding post-mortem management and requests. |
| Must have | A process during user sign up that allows users to specify post-mortem management preferences and designate a next of kin. |
| Should have | A process for restricting access to user data and accounts during and after death verification. |
| Should have | The ability to add metadata to assets for categorisation of user data for post-mortem management. |

Table 9.2: MoSCoW prioritisation of UPAP functional requirements

Non-functional requirements

| Theme | Requirement |
|------------------|--|
| Privacy | Personal and sensitive data must be protected and handled in accordance with applicable legal standards (e.g., GDPR). |
| Usability | Processes must minimise the burden on next of kin by standardising required documentation for death requests and reducing inconsistencies. Service providers should be able to implement UPAP with minimal integration effort. |
| Security | All data exchanges must be encrypted, and strong authentication mechanisms must be enforced for both next of kin and service providers. |
| Interoperability | UPAP should be compatible with a wide range of existing service provider platforms and technical environments. |
| Auditability | All actions taken within the protocol must be traceable for compliance and dispute resolution. |
| Implementation | The protocol should allow each service provider to independently integrate and manage UPAP-compliant post-mortem processes, while adhering to a shared governance and verification framework. |

Table 9.3: Non-functional requirements for UPAP

9.3 Core Principles and Compliance

Relevant legal frameworks considered in UPAP

UPAP draws inspiration from existing legal frameworks with a focus on balancing user privacy and practical post-mortem access. The protocol is designed with the GDPR and China's PIPL in mind, as well as other insight from the legal exploration in chapter 5:

- **GDPR-inspired principles:** While GDPR does not apply to deceased persons according to Recital 27[35], UPAP reflects its core values by supporting user-defined data preferences and secure access control mechanisms as GDPR offers for living individuals.
- **China's PIPL model:** Inspired by Article 49 of China's PIPL, which grants next of kin default rights, UPAP adopts an opt-in model where users are prompted at sign up to actively define next of kin rights.

Security and privacy considerations

UPAP is designed with privacy and security at its core. To protect both the deceased and the surviving NOK, the system incorporates the following safeguards:

- **Granular control:** Users can define who gains access to their data and what actions are permitted (e.g., view, edit, delete, transfer).
- **User-defined boundaries:** Inheritance settings are configurable, allowing individuals to align with personal preferences.
- **Deletion by default:** In the cases where users have not declared their preferences, deletion is chosen based on the findings from section 7.1.

Balancing post-mortem privacy and next of kin access

UPAP applies a deletion-by-default policy in cases where no explicit user preferences have been configured. This default is guided by the following principles:

- **Respect for privacy:** Default deletion ensures sensitive data is not retained unnecessarily after death.
- **User-centric fallback:** In the absence of instructions, deletion protects both the dignity of the user and the NOK from making difficult decisions.
- **Temporary access window:** Before full deletion, data is hidden but available to verified NOK for a grace period.
 - Service providers may configure the window based on policy or jurisdiction.

Approach to cross-jurisdictional legal challenges

UPAP is designed to function across legal landscapes by maintaining a neutral, opt-in structure that allows users to define their own post-mortem preferences, regardless of the current national regulation.

Since there is no harmonised global framework for post-mortem data rights, especially within the EU where the GDPR excludes deceased persons and national laws vary. UPAP temporarily sidesteps this legal inconsistencies by placing control in the hands of the user. However the standard defined by UPAP would have to be updated in the case of law changes in the EU. For death verification, UPAP employs a dual-method strategy, combining an emergency contact with a heartbeat process. The heartbeat process is a periodical verification through notifications to the user and is described in Figure 9.1. This verification ensures that service providers does not have to rely on specific national registries or death databases. This makes it scalable across jurisdictions without requiring integration with local public records.

9.4 Technical Architecture

This section describes the architecture of UPAP, focusing on how it supports death verification, next of kin authentication and designation, and the use of metadata to enrich digital assets with context and user-defined access rules.

Centralised vs decentralised implementation

One of the design decisions in developing UPAP was choosing the right governance model, in order to meet the requirement of independent death verification, as described in section 9.2.

Two approaches were considered and defined as:

Centralised model: This approach uses a single trusted party, such as a public institution, non-profit group, or shared platform, to handle tasks like verifying death, passing that verification to multiple service providers, coordinating access for NOK, and ensuring that participating platforms meet compliance requirements. The centralised party acts as the main contact point for relatives and provides one shared interface that connects to all participating service providers.

Decentralised model: In this model, each service provider is responsible for independently implementing and managing UPAP features. All steps related to post-mortem access, such as identity and death verification, data handling, and legal compliance, are carried out internally. This model allows service providers to tailor their implementation to match legal, technical, or organisational needs.

To support this decision, a comparison table, presented in Table 9.4 to Table 9.8, the pros and cons of each model across a set of criteria, *security*, *compliance*, *user experience*, *cost efficiency*, and *death verification*.

The criteria is defined as:

- **Security:** Evaluates the ability of the model to safeguard post-mortem user data, with attention to control distribution, risk exposure, and vulnerability to system compromise. See Table 9.4.
- **Legal compliance:** Assesses how readily each model can operate within varying legal frameworks, including data protection and inheritance regulation. See Table 9.5.
- **User experience:** Considers the level of effort required by users and next of kin, including the clarity, accessibility, and consistency of the post-mortem management process. See Table 9.6.
- **Cost efficiency:** Compares the implementation and maintenance costs of each model, particularly in relation to resource demands on service providers. See Table 9.7.
- **Death verification:** Examines the mechanisms used for death verification, focusing on reliability, scalability, and the potential for false positives. See Table 9.8.

| Criteria: Security | |
|--|---|
| Centralised | Decentralised |
| <p>Pros:</p> <ul style="list-style-type: none"> • Uniform security standards across providers • Location in the EU ensures alignment with GDPR <p>Cons:</p> <ul style="list-style-type: none"> • Single point of failure if central entity is compromised • Security bottleneck due to reliance on one party | <p>Pros:</p> <ul style="list-style-type: none"> • Full control over encryption and data handling • Eliminates central point of failure <p>Cons:</p> <ul style="list-style-type: none"> • High cost for implementing local security measures • Potential legal mismatch with different jurisdictions |

Table 9.4: Security comparison between centralised and decentralised UPAP models

From a security perspective, centralised systems benefit from consistent enforcement and alignment with frameworks like GDPR, but create a single point of failure and centralise risk. The decentralised model distribute risk and offer greater control, yet demand more effort and infrastructure from individual service providers, as detailed in Table 9.4.

| Criteria: Compliance | |
|--|--|
| Centralised | Decentralised |
| Pros: <ul style="list-style-type: none"> • Only one party requires legal certification Cons: <ul style="list-style-type: none"> • Public trust may be lower in centralised oversight • Risk of lobbying by dominant platforms | Pros: <ul style="list-style-type: none"> • Trust remains with service providers • Avoids external regulatory influence Cons: <ul style="list-style-type: none"> • Legal compliance becomes service provider specific • High effort for cross-border compliance |

Table 9.5: Compliance comparison between centralised and decentralised UPAP models

In terms of compliance, centralised approaches simplify oversight by combining legal responsibility, though this centralisation may lower trust and increase susceptibility to external influence. Decentralised models preserve platform autonomy but impose legal obligations on each provider, as shown in Table 9.5.

| Criteria: User Experience | |
|---|---|
| Centralised | Decentralised |
| Pros: <ul style="list-style-type: none"> • Single interface to manage all accounts • One contact point for next of kin Cons: <ul style="list-style-type: none"> • High integration effort across platforms | Pros: <ul style="list-style-type: none"> • Compatible with existing legacy systems • Customisable post-mortem preferences Cons: <ul style="list-style-type: none"> • Setup must be repeated per platform • Next of kin handle separate verification processes |

Table 9.6: User experience comparison between centralised and decentralised UPAP models

From a user experience standpoint, centralised systems streamline the post-mortem process by providing a unified interface, making it easier for NOK. However, this comes at the cost of complex integration. Decentralised setups allow more customisation but require greater effort from both users and their families, as seen in Table 9.6.

| Criteria: Cost Efficiency | |
|--|---|
| Centralised | Decentralised |
| Pros: <ul style="list-style-type: none"> • Shared compliance and administrative burden Cons: <ul style="list-style-type: none"> • Requires coordination across jurisdictions • Unclear obligations for non-EU providers | Pros: <ul style="list-style-type: none"> • No need for third-party involvement Cons: <ul style="list-style-type: none"> • Higher setup and maintenance costs per provider |

Table 9.7: Cost efficiency comparison between centralised and decentralised UPAP models

Regarding cost efficiency, centralised models allow for shared infrastructure and regulatory compliance, particularly in transnational regions like the EU. In contrast, decentralised models avoid third-party reliance but result in higher implementation and operational costs for each service provider, as illustrated in Table 9.7.

| Criteria: Death Verification | |
|--|--|
| Centralised | Decentralised |
| Pros: <ul style="list-style-type: none"> • Verification via national identity systems • Single death event applies across all service providers Cons: <ul style="list-style-type: none"> • One false positive can impact every linked service | Pros: <ul style="list-style-type: none"> • Detection can rely on platform-specific activity signals • Verification can be adapted to data type Cons: <ul style="list-style-type: none"> • Death may be recognised inconsistently across platforms |

Table 9.8: Death verification comparison between centralised and decentralised UPAP models

In the context of death verification, centralised systems benefit from standardised access to national identity databases, enabling consistent verification across platforms. Yet this standardisation means that a single false positive could spread across all connected service providers, potentially triggering unintended data release or deletion. Decentralised models offer flexibility and contextual adaptation, but risk inconsistency and verification errors, as discussed in Table 9.8.

Final decision and justification

Based on the trade-offs outlined in the comparison tables, the decentralised model was chosen as the architectural basis for UPAP. Although the centralised model offers simpler oversight and user interaction, it depends on a neutral third party, which does not exist today and would require political, financial or legal backing. This makes it difficult to implement in the short term. The decentralised model allows individual service providers to adopt the protocol independently. While it introduces higher operational effort, it avoids single points of failure, supports legal flexibility, and is more realistic to implement under current conditions.

Death verification process

A fundamental challenge in digital legacy management is reliably verifying the death of a user when notified by a third party. UPAP aims to address this by reducing the administrative burden on NOK while minimising the risk of false positives. It is essential to ensure that reported deaths are genuine, preventing adversaries from fraudulently triggering death events and activating post-mortem processes on user accounts. To develop effective practices for service providers, it is necessary to first examine how death events are currently verified and managed.

Current practices for verifying death events

The analysis of service providers in chapter 6 examined how NOK can gain access to an account, request account deletion, or what occurs when no external party takes action. These findings describes gaps and issues, in the current practices of service providers, informing a proposal of a new process.

The findings include:

- The process for NOK access varies significantly across platforms.
- As shown in Figure 6.1, 14 out of 20 providers do not suspend inactive accounts, meaning accounts belonging to deceased users may remain active and potentially at risk.
- The overview in Figure 6.2 revealed that only 7 of 20 platforms offer a legacy contact feature, with considerable variation in the level of access provided.
- Gaining access to an account is dependent on legal documentation, often requiring one or more of the following:
 1. Death certificate
 2. Proof of relationship (e.g., marriage certificate, birth certificate, will, estate letter, power of attorney)

3. Probate certificate, court order, or letter of administration
4. Valid photo ID of the requester (passport, driver's license, etc.)
5. Account details (email address, username, profile URL)
6. Obituary or memorial card
7. Billing or payment information
8. Legal proof of authority (executor/administrator documentation)

Proposed process for verifying death events

UPAP proposes a solution that builds upon and is inspired by the current practices of service providers with established post-mortem policies.

UPAP enforces the assignment of an emergency contact during the initial user sign up. By ensuring that an emergency contact is available from the outset, UPAP enables the contact to be notified and involved throughout the entire death verification process.

In addition, UPAP introduces a heartbeat process. Much like a regular health check, the heartbeat process periodically verifies user activity. When combined with the submission of a death certificate, this dual approach reduces the risk of false positives.

It is important to note that the analysis in chapter 6 did not examine how service providers currently validate the authenticity of death certificates due to limited information available from providers. Therefore, the heartbeat process is designed as a complementary layer to existing death certificate verification procedures, rather than a replacement. Verification of death certificates would require an authorised entity in each country, but this could potentially be unified across Europe using eIDAS 2.0. This is discussed in section 10.3 about future directions for the research.

The heartbeat process leverages both activity logs from the service provider and direct notifications to the targeted user. For the process to be considered successful, there must be no recorded activity from the user. If any user activity is detected during the verification period, the process is stopped and the activity is investigated, as it may indicate either a false request or a potential account compromise.

Additionally, the heartbeat process initiates a strategy, where notifications to the user are sent at increasing intervals to reduce notification fatigue and avoid overwhelming the user. The user may receive notifications by email, SMS, or phone call, depending on the severity level of the service provider. Another success criterion for the heartbeat process is that the user does not respond to any of the notifications. The specific notification intervals are not set in this report, as there is currently no established standard for the optimal duration.

The mapping of severity levels to notification channels, as well as the corresponding verification requirements for NOK, is shown in the following Table 9.9. An additional row is included to indicate requirements that are common to all severity levels.

| Severity level | Verification requirements | Notification channels |
|----------------|---|---|
| All | Official death certificate Valid photo ID of requester Account details Proof of relationship | |
| Critical | Preassigned emergency contact | Mail SMS Phone call Activity log |
| High | Preassigned emergency contact | Mail SMS Phone call Activity log |
| Medium | No additional requirements | Mail SMS Activity log |
| Low | No additional requirements | Mail Activity log |

Table 9.9: Mapping of severity levels to notification channels and verification requirements for next of kin. The table includes a row for requirements common to all severity levels.

Figure 9.1 shows the heartbeat process when all notification channels are included.

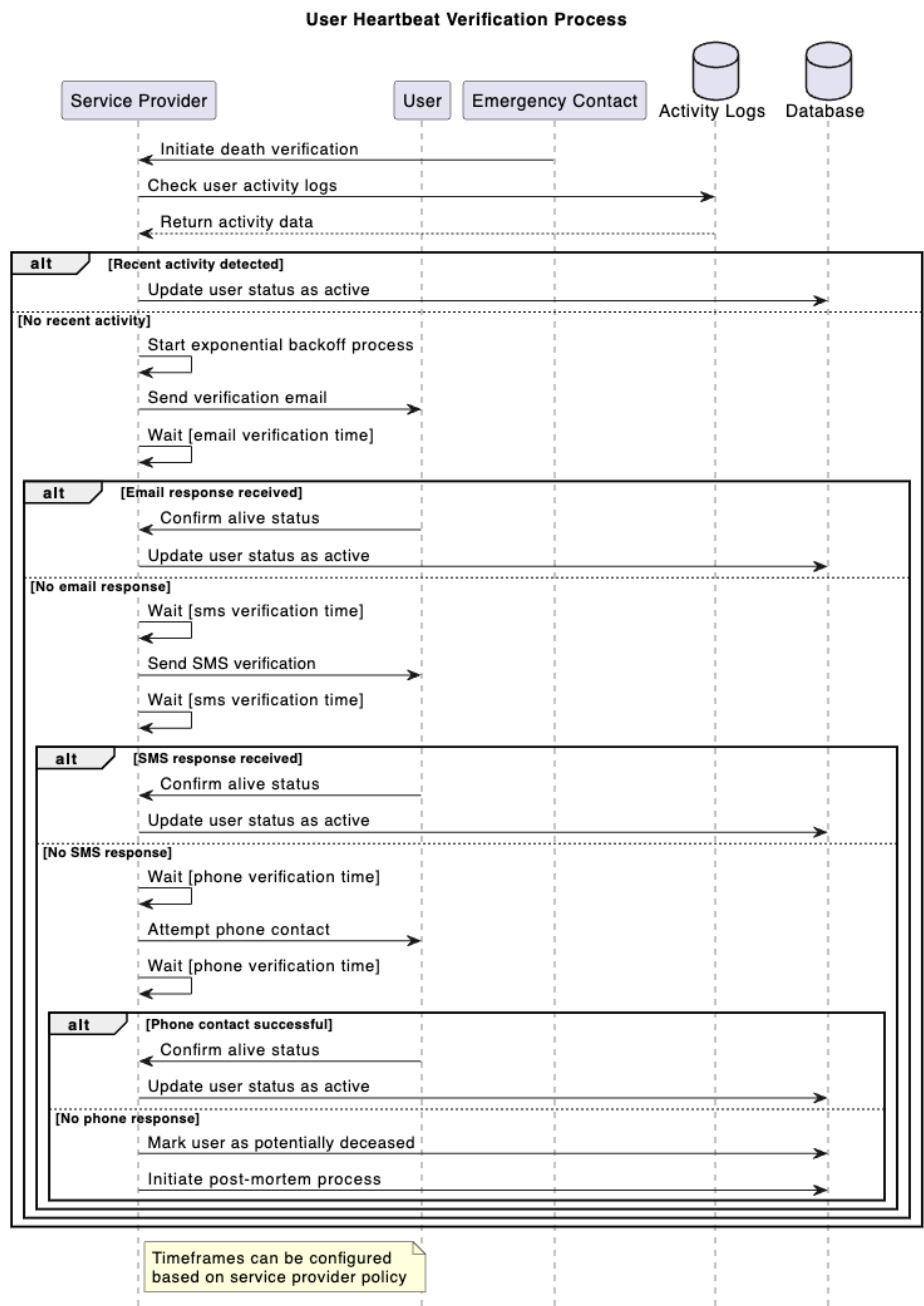


Figure 9.1: Sequence diagram showing the death verification process using the heartbeat method.

- 1. **Process initiation by emergency contact:** The emergency contact submits a request to the service provider to initiate the death verification process.
- 2. **Activity log check:** The service provider checks the activity logs of the use to deter-

mine if there has been any recent activity.

3. **Recent activity detected (alternative path):** If recent activity is found, the user is marked as active, and the process ends.
4. **No recent activity – start heartbeat process:** If no recent activity is detected, the service provider starts the heartbeat process using an the following strategy:
 - **Email notification:** A verification email is sent to the user. If the user responds, their status is updated to active and the process ends.
 - **No email response:** If there is no response within the set timeframe, an SMS verification is sent. If the user responds, their status is updated to active and the process ends.
 - **No SMS response:** If there is still no response, a phone call attempt is made. If the user responds, their status is updated to active and the process ends.
 - **No phone response:** If there is no response to any notification, the user is marked as potentially deceased and the post-mortem process is initiated.

Approach to next of kin designation during account creation

The sequence diagram in Figure 9.2 illustrates the flow for configuring emergency contacts and post-mortem data management preferences during the user sign up process with a service provider. The process is described as follows:

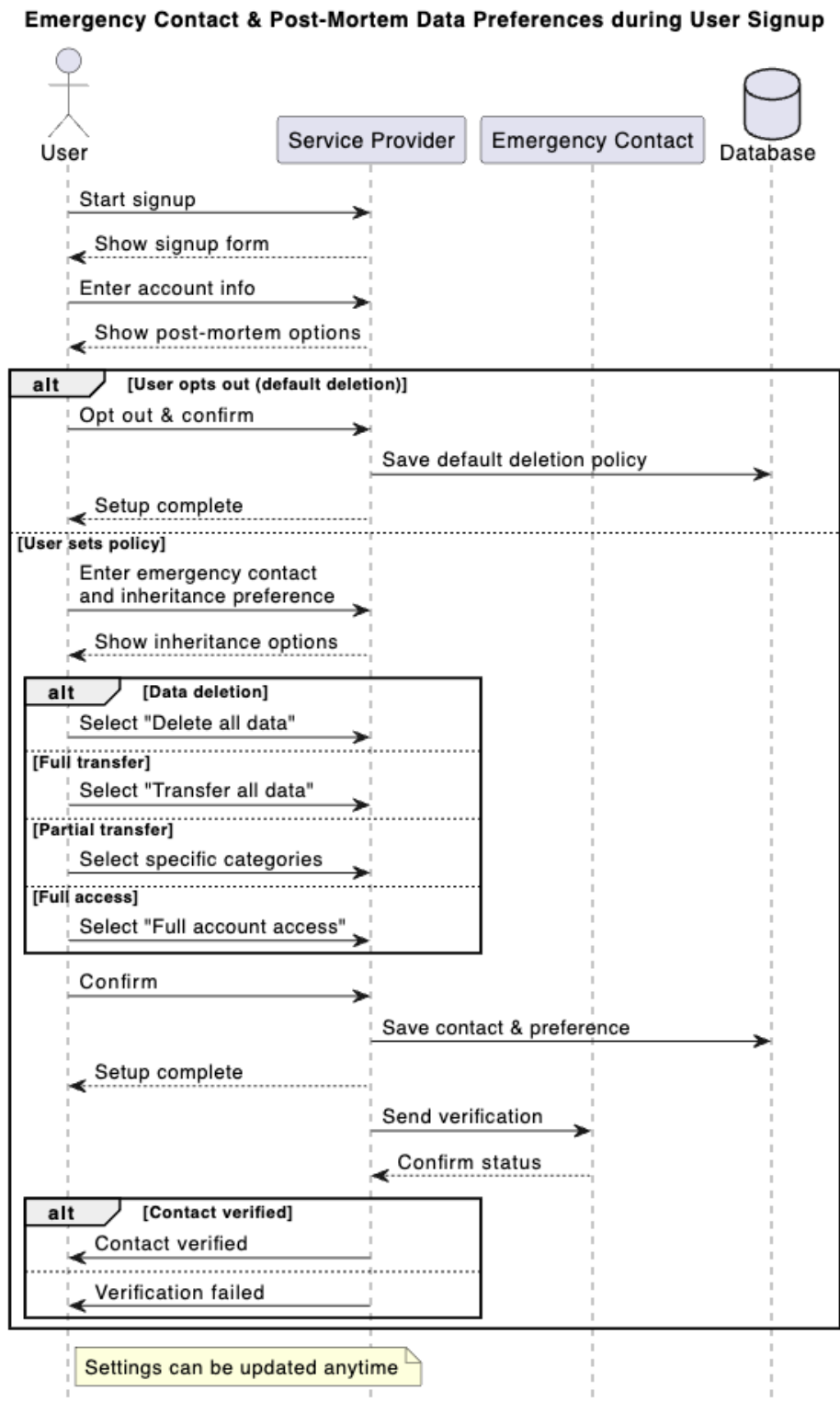


Figure 9.2: Sequence diagram showing the workflow for configuring emergency contact and post-mortem data management preferences during user sign up.

1. **User onboarding:** The user initiates the sign up process, completes the account information form, and is presented with post-mortem data management options.
2. **Custom post-mortem preferences:** Users can choose to opt-out or enter an emergency contact and select their preferred inheritance option from the following:
 - **Deletion by default:** Users who do not wish to specify preferences may opt out, resulting in the default deletion policy.
 - **Alternatively, choose a policy**
 - Delete all data after death (with assigned emergency contact)
 - Transfer all data to the emergency contact
 - Transfer only specific categories of data
 - Grant full account access to the emergency contact
3. **Confirmation and verification:** Once a preference is selected, the user confirms their choice. The service provider stores the emergency contact information and the selected policy. A verification message is then sent to the emergency contact to confirm their willingness and availability.
4. **Contact verification:** If the emergency contact successfully verifies their identity and agrees to the role, the setup is completed. Otherwise the verification fails.

This flow ensures that users can proactively determine the fate of their digital assets and designate a trusted party to manage their data after death. Users retain the ability to update their post-mortem settings, and emergency contacts at any time through their account settings.

Existing users will be presented with a similar process when logging in for the first time after UPAP is implemented, ensuring consistency across both new and current accounts.

In the case where no emergency contact is specified, UPAP requires that the system defaults to inactivity-based deactivation policy, typically resulting in account suspension or deletion after a defined period of inactivity.

Authentication of next of kin

Upon user registration, one or more emergency contacts are designated. Assigned contacts is required to approve their willingness to take on this responsibility.

When NOK notifies the service provider of the death of the user, they must submit a valid government issued photo ID as part of the authentication process. UPAP only requires the service provider to confirm the identity against the information given for the emergency contact at sign up and to rely on their existing identity verification measures.

If the identity of the requester matches the pre-assigned emergency contact, the system proceeds to validate the death event using the heartbeat process.

Enhancing digital asset context through metadata

UPAP proposes a use of metadata to support user in granular asset selection in digital legacy management. Rather than imposing a solid, one-size-fits-all model, the protocol requires that service providers develop a metadata framework that fits the structure and context of the data on their platforms. The core idea is to give users the ability to label their digital assets according to personal wishes about post-mortem access.

Example: Users of Google Drive can attach metadata to files and folders with *Family*, *Personal* and *Work*. In their preferences the data labelled *Family* will be sent to NOK, *Work* to a colleague and the rest is marked for deletion.

Recognising the diversity of digital platforms, UPAP does not prescribe exact labels, but instead encourages service providers to interpret and implement metadata in a manner that makes sense for their service and the data it holds. This approach respects individual differences and the variety of metasoul people have, making it possible for users to exercise control over what lives on in their metasoul.

9.5 Implementation considerations for service providers

How service providers can implement UPAP

Implementing UPAP requires resources across technical, legal, and operational domains.

To implement UPAP, service providers need to implement changes to their existing systems and policies. This includes introducing the additional step during sign up for setting emergency contacts and digital legacy preferences. Metadata tagging should also be enabled, allowing users to label digital assets for granular control.

In terms of death verification, a combination of the service providers existing death certificate verification and the heartbeat process of UPAP, visualised in Figure 9.1, should be implemented.

From a security perspective, providers need to ensure encrypted handling of sensitive data, particularly when NOK request deletion or access. This may involve additional compliance work, internal audits, and updates to privacy policies. Operationally, customer support staff must be prepared to assist grieving families, manage requests, and handle disputes. Finally, providers must allocate resources for long-term maintenance to ensure UPAP processes stay up to date and secure.

Incentives for service provider participation

By adopting UPAP, service providers demonstrate a commitment to ethical data management and user trust. The protocol allows providers to offer clear and structured processes for handling post-mortem data, something that is currently inconsistent or missing across most platforms. This not only supports families during a vulnerable time but also reduces reputational and legal risk in the absence of clear regulation. While UPAP is voluntary today, it anticipates future legislation similar to how GDPR reshaped data privacy.

9.6 Proposal for validation and testing metrics

The validation and testing phase is central to understanding whether the UPAP effectively addresses the real-world needs and challenges of digital legacy management. The process relies on several metrics and ethical guidelines, aimed at ensuring the protocol is both effective and sensitive to the needs of users. While this section lists the metrics proposed, no testing of UPAP was carried out during this thesis.

Metrics for validation

The following statistical metrics could be used to evaluate the success of UPAP and its implementation by service providers:

- **Adoption by service providers:** The number of service providers that have implemented UPAP, and whether this was achieved without major issues.
- **Accuracy of death event handling:** The number of successful death verifications, and the rate of false positives, meaning cases where a death was wrongly registered. The accuracy of death event handling can potentially be evaluated through audit samples, tracking appeals and reversals.
- **Request processing time:** The time required to process requests related to post-mortem data management.
- **User adoption:** The proportion of users who choose to set up an emergency contact and define their post-mortem preferences.
- **Next of kin satisfaction:** Feedback is collected to determine whether the system helps relieve frustration for NOK during the grieving period.

These metrics provide an outline of what measures could be taken to achieve both reliability of technical operations and the overall acceptance among users.

Ethical considerations

Following is the ethical aspects that should be integrated into the validation process of UPAP:

- **Respect for user wishes:** Ensuring that the preferences set by users before death are followed.
- **Verification of death events:** Applying dual-factor checks to confirm death events and avoid accidental or malicious actions, such as attacks on living users.
- **Transparency and user control:** Making sure users understand their choices and can update their wishes over time.
- **Consideration for grieving contacts:** Recognising that emergency contacts may be in a period of grief, and aiming to reduce additional stress or frustration during the process.

By applying these validation metrics and ethical guidelines, the evaluation of UPAP aims to confirm both its technical strength and its practical value for all participants involved.

Chapter 10

Discussion

This chapter reflects on the research findings and examines their implications for improving post-mortem data handling. It considers how more secure, transparent, and user-friendly solutions, aligned with legal standards and platform practices, as outlined in section 1.2, can help address existing gaps in digital legacy management.

The research started by investigating current practices, challenges and expectations around post-mortem data management, with the aim of laying a foundation for the design of a standardised protocol, UPAP, presented in chapter 9. Drawing on insights from legal frameworks, service provider policies, and user experiences, this discussion explores the broader significance of the results by examining the findings, major gaps in the current landscape, and evaluating the proposed solution.

10.1 Recurring themes and proposed solution

10.1.1 User awareness, behaviour, and barriers in digital legacy planning

Although digital technologies have become deeply embedded in daily life, the vast majority of users remain unprepared for what should happen to their digital assets after death. Findings from the survey, analysed in section 7.1, reveal a striking gap in both awareness and planning. A total of 85.7% of respondents had never encountered the term *digital legacy*, while 76 of the 140 respondents reported that they had never considered the fate of their data after death. 130 of the respondents reported to not have taken any action on their digital legacy with only 10 having implemented any measures, and these were largely informal, such as writing down passwords or sharing them with relatives.

While these methods may appear practical, they are inherently insecure and conflict with basic cyber security principles. In addition to the unawareness, the survey analysis also displayed a lack of knowledge and combined with the findings in the service provider

analysis, in chapter 6, displaying a lack of clear approaches to post-mortem planning, the users are left with limited ways to manage their legacy.

This behavioural pattern is consistent with what Holt et al. describe as the post-mortem privacy paradox: *"users recognise the importance of posthumous data planning but refrain from taking concrete steps"*. [38] Grimm and Chiasson likewise found that most individuals had never given serious thought to their digital footprint in a post-mortem context. [37]

The lack of planning carries multiple risks, including loss of meaningful data, potential privacy breaches, and emotional distress for next of kin. There is a clear need for structured, user-friendly solutions that support both awareness and action. UPAP, the protocol proposed in chapter 9, addresses this need by encouraging users to actively define how their data should be handled and by whom. In addition, educational campaigns and supportive policy frameworks could help raise awareness and normalise digital legacy planning, as Astrid Waagstein mentioned during an interview, described in section 7.2, and as Öhman and Floridi argue, digital death should be treated as a public matter of ethical and informational governance, comparable in awareness to topics like organ donation and inheritance law. [61]

This gap between user intentions and available support prompts the next theme: whether current post-mortem data solutions align with user needs.

10.1.2 Bridging the gap between user needs and post-mortem data solutions

As the digital-native generation continues to grow, so too does the need for clear and structured approaches to handling post-mortem legacies. While users are building up their digital footprint, most service providers have yet to adapt their systems. A central point for discussion arises: *Do existing post-mortem solutions reflect what users actually need and want?*

The results from the user survey, in section 7.1, reveal what preferences users have regarding the fate of their digital assets. When asked how they would prefer to handle their digital legacy, 32.9% of participants indicated that they would like all accounts and data to be permanently deleted. Another 23.5% preferred to give full access to a trusted individual, while 20% wanted their account deleted but selected data transferred to NOK. These responses point to a clear demand for flexible options that support both deletion and controlled delegation. However, very few platforms currently support this level of granularity.

The analysis of service providers, in chapter 6, indicate that the 20 service providers shows substantial variation in how platforms manage post-mortem legacies. While 14 providers offer some form of official documentation, the level of detail, clarity, and accessibility differs greatly. Only a small group of providers, including Google, Apple, Facebook, and certain password managers, offer features for assigning NOK to manage the account post-

mortem. The majority either lack dedicated procedures or have unclear and difficult requirements, particularly in the case of NOK account access. Platforms such as WhatsApp, Signal, Steam, and Snapchat provide minimal or no guidance, often leaving accounts indefinitely active. Inactivity-based deletion is also rare, implemented in only 6 out of 20 cases.

This mismatch creates significant challenges for grieving families, who may need to provide extensive documentation during an already difficult time. It also leaves users with limited means of proactively managing their digital presence after death. This might explain why informal solutions, such as sharing credentials, remain a common workaround despite the associated security risks.

The contrast between user expectations and current service provider capabilities highlights the need for more uniform and user-centric solutions. UPAP contributes to this vision by offering a protocol that enables service providers to reach a consistent standard by embedding user choice directly into account configuration.

10.1.3 Legal Gaps and the need for harmonised regulation

The legal regulation regarding post-mortem legacies is still inconsistent across countries. At the European level, the GDPR does not apply to deceased people, leaving it up to each Member State to decide how such data should be handled. As discussed in chapter 5, this has led to different national approaches. Norway and Sweden have no specific laws addressing digital legacy. Norway provides some guidance in relation to workplace data, and Denmark allows certain data protection rules to apply for up to 10 years after death.

Outside Europe, China's PIPL stands out by granting NOK a clear legal basis for post-mortem data management. As noted in chapter 5, China's approach to privacy differs significantly from the EU and scores low on several privacy indices[5, 21, 65]. This raises the question: *How is it that China, despite its criticised approach to privacy, still includes post-mortem data management in the PIPL?* The answer may lie in cultural attitudes toward death and highlights the need to consider such differences in designing post-mortem frameworks.

The lack of legal regulation around post-mortem data creates practical challenges for users and their families. Without clear obligations, service providers are not required to support digital legacy planning. As shown in the survey results, in section 7.1, and supported by interview findings, in section 7.2, this often leads to confusion and inconsistent procedures when families attempt to access or close the accounts of a deceased relative.

To address this, coordinated regulation at the EU level is needed. Defining basic rights and responsibilities for handling personal data after death would create consistency across platforms and give systems like UPAP a clear legal foundation, moving implementation by service providers beyond voluntary use.

The project eIDAS 2.0 could support digital legacy management by enabling cross-border

verification of death certificates. This would help service providers act on user instructions more reliably and ease the burden on families. The potential role of eIDAS 2.0 is discussed further in subsection 10.3.1.

10.1.4 Alternative solutions and design justification

The Unified Post-Mortem Access Protocol is designed as a flexible standard that service providers can implement in their own systems. It is not a tool or platform, but a set of rules and procedures to help manage digital accounts after death.

As described in chapter 9, UPAP is designed with decentralisation in mind. However, the protocol is flexible and could be adapted to support a centralised setup if needed.

In a centralised model, a trusted third party, such as a public agency or non-profit, would be responsible for verifying deaths and managing access requests. This could reduce the workload and risk for service providers but would likely require legal and financial backing or shared governance to succeed.

For reference, the comparison of the two approaches is described in section 9.4.

Some large platforms already offer legacy features. These tools can work well within that one platform. But they are not coordinated, and they do not support consistent death verification. Families must learn different rules for each service, and there is no shared way to prove someone is dead.

UPAP was designed to be practical and implementation should be available for service providers with minimal adjustment to their current infrastructure. UPAP aims to be practical by:

- Working with or without new laws.
- Letting users stay in control.
- Be adaptable to different platforms and countries.
- Could connect with systems like eIDAS 2.0 to verify deaths more easily, as described in subsection 10.3.1.

To understand whether UPAP is the right solution in practice, it must be tested with real users and service providers. However this is not done in the scope of this thesis, but metrics for its success is prepared and further discussed in subsection 10.3.2.

10.2 Limitations

10.2.1 Legal framework analysis

There is a clear lack of laws and regulations that deal specifically with digital legacy management. The thesis does not aim to give legal interpretations, as we are not legal experts. Instead, the focus was on highlighting the gaps and uncertainties in this area. The legal analysis focused on Danish law and selected international frameworks, which scoped the legal perspective. As explored in the thesis the legal aspect of the topic is still underdeveloped and that yielded a challenge in findings comprehensive resources.

10.2.2 Service providers analysis

The analysis of service providers presented in this thesis relies on a combination of official, secondary, and third-party sources, including terms of service, help center documentation, and official platform guidelines, which has been stated in Table 6.2. While this method offered a broader pool of resources, it came with limitations in reliability and completeness. Many platforms do not make their post-mortem data policies explicit, and those that do required deep exploration of their complex policies. As a result, the accuracy of the findings could have been affected by the clarity and transparency of each policy available.

To strengthen the analysis, we considered reaching out directly to service providers. However, this aspect was deprioritised due to unsuccessful outreach attempts. Three outreach attempts were made to MitID[57] (Denmark's national digital identity provider), a digital legacy service provider, and the Ministry of Digitalisation[19], specifically the unit responsible for the CPR registry. Either no response was received, or the replies lacked sufficient detail to be included in the analysis. This experience was also a challenge for the interviewees, when they reached out to official Danish authorities, that reported either no or insufficient answers.

10.2.3 Interview handling

During the interviews, written notes were used to summarise the conversations instead of recording audio. This decision was made to respect for the sensitivity of the topic, as many of the interviewees shared personal experiences involving the death of close relatives or colleagues. The aim was to create a setting that felt safe and respectful, avoiding any additional discomfort that recording might cause. Audio recordings would have enabled a more in-depth analysis since all details would be available.

10.2.4 Proof of concept

The proposed solution in this thesis is limited to a POC rather than a fully implemented and deployed system. While the POC effectively illustrates the structure, logic, and in-

tended functionality of the UPAP, it remains a conceptual prototype. This means that the solution has not been tested in real-world environments, nor has it received feedback from actual users or service providers. The lack of testing and stakeholder feedback leaves room for uncertainty in areas like user experience, technical implementation challenges, and service provider adoption. Future work should focus on refining the system through iterative testing and dialogue with relevant stakeholders.

10.3 Future work

10.3.1 Verification of death certificates

An area for future work of UPAP, is the automation and standardisation of death certificates verification across national borders.

A potential solution would involve service providers gaining automated access to digitally signed death certificates, issued by national authorities, potentially through eIDAS 2.0 and the EU Digital Identity Wallet. This would support cross-border verification in the EU which is explored in subsection 5.4.1.

This could enable:

- Fast and secure validation of death status directly from trusted registries
- Reduced administrative burden on NOK and service provider
- Improved protection against misuse and false death requests

Future work should examine the technical possibility, legal implications, and privacy protections, required to integrate this process directly into the UPAP access flow.

10.3.2 Implementing and testing a MVP of UPAP

Another important direction for future work is developing and testing a version of UPAP which can be put into the real world. While this thesis outlines the conceptual architecture and flow of the UPAP, no actual implementation in practice has been developed or evaluated.

The focus should be on an implementation of the protocol that can be tested with both service providers and end users, this could make it possible to:

- Evaluate the technical possibility of integration with existing service provider infrastructures
- Conduct user testing to assess the protocol, its ease of use, clarity and emotional impact, based on the metrics from section 9.6

- Gather feedback on user experience, including how NOK interact with access requests, and how users perceives post-mortem data handover mechanisms

This MVP would validate UPAP in real world conditions and bridging the gap between protocol design and practical implementations.

10.3.3 Threat modelling the post-mortem landscape

An important area is the threat modelling of post-mortem management. As UPAP propose a framework for handling access to user data after death, it is crucial to understand how the protocol might be exploited by malicious actors. Additionally, the findings from chapter 6 indicate that many service providers may hold accounts belonging to deceased users, potentially creating an attack surface for adversaries.

Future work should explore what attack vectors may exist, particularly for adversaries targeting account of deceased individuals. This could include unauthorised access to sensitive data, impersonation of the deceased, or manipulation of digital content to distort their legacy.

During the interviews, Astrid Waagstein, PhD in post-mortem data rights, from the qualitative interview, in section 7.2, expressed a concern about the potential for someone to *"Destroy one's legacy"* by providing incorrect information or altering personal data after death. This highlights the importance of evaluating not just technical security, but also reputation and dignity risks that could arise from compromised post-mortem systems.

A threat model could help identify:

- Weak points in authentication and death verification logic.
- Scenarios involving identity hijacking, and manipulation of digital remains.
- The impact of insecure service provider practices after death.
- The threat actors that could be involved in the post-mortem data landscape

By analysing these risks future implementations of UPAP can be designed with stronger safeguards.

10.4 Ethical considerations

A limitation in the development of the proposed solution UPAP is the ethical complexity involved in managing digital legacies. At its core, the challenge lies in balancing two opposing user rights: the right to be forgotten and the right to be remembered. The survey analysis, in section 7.1, showed that many users prefer complete data deletion after death, while others may want certain digital assets preserved. This raises significant

ethical questions about how digital systems should interpret and act on the wishes of an individual, particularly when those wishes are unclear.

The ethical challenge deepens when designing for users who can no longer represent themselves. As the research has indicate, digital legacies are unique and should be handled accordingly. However, digital systems require standardisation to work at scale. Ethically, this raises the concern: *Can a uniform protocol ever truly respect the uniqueness of an the metasoul of an individual?*

Chapter 11

Conclusion

This thesis explored the increasingly important yet under-explored domain of digital legacies and post-mortem data rights. It aimed to improve digital legacy management by proposing a conceptual protocol, Unified Post-Mortem Access Protocol, informed by legal frameworks, current service provider practices, and user insights, to address the central question:

How can digital legacy management be improved through the development of a conceptual solution that ensures secure, clear, and user-friendly handling of post-mortem data, in alignment with existing legal frameworks and the practices of digital service providers?

The research followed a threefold methodology, combined of a legal exploration, service provider analysis and collection of user insights and experiences.

The legal exploration aimed to access legal coverage of post-mortem data rights and access for next of kin. The exploration focused on Danish law, fellow Scandinavian countries, and the protections GDPR offers. In addition the exploration covered the EU initiatives, eIDAS 2.0, the European Law Institute.

The service provider analysis included policies from 20 platforms across a range of digital identity types. The analysis focused on exploring official post-mortem policies and the measures available to users and NOK for protecting their data, outlining the requirements for carrying out such actions.

The third part involved data collection through both a quantitative survey and qualitative interviews. The quantitative survey, yielding 140 responses, was designed to understand users awareness, behaviour and experiences in managing digital legacies. Additionally a series of qualitative interviews were conducted to to better understand the practical and emotional aspects of digital death through personal experiences.

The findings from the research was used as the basis for an internal workshop to design

and develop UPAP, a standardised framework for service providers in managing digital legacies.

11.1 Concluding summary

This research uncovered several recurring themes and structural gaps in how post-mortem data is understood and handled, across user experiences, legal frameworks, and service provider practices. The following summary presents the main findings in the three categories.

11.1.1 Assessing legal readiness for post-mortem management

Recital 27[35] of the GDPR explicitly states that its regulations does not apply to deceased individuals, but rather leaves post-mortem data protection to national legislation.

In the Danish context, data protection extends beyond death. As stated in §2, subsection 5 of the Danish Data Protection Act[49], extends GDPR and the rights of the individual for 10 years after their passing.

Norway and Sweden, excludes deceased individuals from their scopes. However in Norway, the Norwegian Data Protection Authority[13] provides guidelines for post-mortem handling of employees, emphasising privacy, minimal access, and oversight to protect both the deceased and living individuals.

The EU projects included in the exploration, while not directly focused on post-mortem data, influence how digital legacies might be managed in the future. eIDAS 2.0[25] introduces the European Digital Identity Wallet, which could support secure storage of post-mortem instructions, identity-linked permissions, and legal documents. European Law Institute (ELI)[29] has launched a project to harmonise digital inheritance and emphasises treating digital assets as inheritable property and addresses recurring challenges such as jurisdictional conflicts, contract restrictions, and post-mortem privacy concerns.

11.1.2 Lack of standardisation for service providers

The service provider analysis revealed significant inconsistency in post-mortem data management. 14 of the 20 providers probed offered post-mortem guiding, however the clarity, accessibility, and level of detail vary considerably.

In terms of the actions available for the users and their NOK, seven providers offers the user with solution for planning their digital legacy through pre-assignment of a legacy contact and three providers allow for post-mortem access for NOK through a legal process. This leaves 10 providers offering no access, regardless of pre-planning or legal action. For these, the only available option would be to request deletion or deactivation through a legal process, a feature still not supported by 3 of them.

However, the difference in service provider approaches continues in the specific ways they offer their post-mortem solution, in terms of the legal documentation required from the NOK, which imposes a substantial burden on grieving relatives.

Inactivity-based deletion is rare, used by only six platforms. As a result, many accounts may stay active long after the death of their owner, leaving their data exposed and without the possibility of intervention in case of leaks or attacks.

As not all providers pose the same level of risk, a risk assessment was conducted to determine their severity level based on the data they hold and the access they provide, in order to define the level of responsibility they should uphold in relation to metasoul management. The assessment rated password managers and account or email services as critical due to their sensitivity and central role in accessing other platforms.

The risk assessment was used to recommend proportionate standards and responsibilities through UPAP.

11.1.3 Findings from survey and interview analysis

The findings through the user survey and interviews, revealed a clear lack in awareness and metasoul planning among Danish residents.

120 of respondents reported not knowing the term *digital legacy*, and 130 had taken no action regarding their metasoul. The biggest reasons for the lack of action was simply not considering the topic, reported by 76, or not knowing what to do, reported by 41. Even the 10 respondents that had taken action reported usage of manual methods, including sharing and writing down passwords, which contradicts secure practices. When asked what the respondents preferred in terms of the management of their digital legacy, 49 reported that they wished for full deletion of their data, and 33 wished to appoint a NOK for full-access.

During the interviews, recurring themes emerged, including immediate account lockdown by government services and difficulty gaining access afterwards. Attempts to contact public institutions often resulted in inconsistent replies or no response at all, especially in a case involving death abroad, where death certificates could not be verified. This left the digital legacies of the deceased active despite their passing. Across interviews, there was a clear sense of frustration and powerlessness in handling digital legacies.

11.2 Proposed solution

The Unified Post-Mortem Access Protocol (UPAP), is proposed as a conceptual solution to the fragmented and inconsistent handling of digital legacy across service providers. To achieve this, UPAP prompts users to actively define their preferences and emergency contacts. It also introduces a heartbeat process, an activity and notification, based check,

designed to complement existing death verification methods and reduce false positives, without requiring third-parties verification.

11.3 Impact and Contributions

This thesis contributes to the field of digital legacy management through a cross disciplinary lens by highlighting legal, technical and human facing challenges, particularly in a Danish context.

The thesis also proposes a practical contribution, UPAP, which outlines procedural and core concepts for service providers to implement post-mortem legacy management and thereby achieve a more consistent and user-centric handling of digital legacies.

Lastly, the research identifies a notable gap in public awareness and behaviours. Many individuals, despite their acknowledgement of the issue, remain unsure of their rights or options, and many service providers still treat death as an operational exception rather than a user journey worth designing for.

11.4 Future research directions

11.4.1 Commercial motives

A valuable direction for future research is to examine whether service providers have any incentives for keeping post-mortem data rather than deleting it. In terms of advertising, some platforms use algorithms that learn from user behaviour to deliver more effective ads. This prompts the questions of whether post-mortem data of users, such as likes, clicks, and viewing habits, could be useful, and therefore the data is retained to help platforms improve their ad performance and increase revenue. For example, the advertising tools of Facebook, are improved by user data to make ads more relevant, and the questions remains if they would profit from using post-mortem user data.[2]

Another potential for commercial gain is the use of post-mortem data in the training of artificial intelligence, which would raises questions about consent, transparency, and the long-term use of post-mortem data.

11.4.2 Psychological aspect

Another direction for future research is to explore the psychological obstacles related to digital legacies. People often find difficulty in dealing with the topic of death, as it feels distant and uncomfortable, which might their decision in taking action. This presents a research opportunity in answering how individuals can be encouraged, on a psychological level, to prepare for the management of their digital legacy.

11.4.3 Cultural considerations

Another area relevant to future research is the cultural aspect of digital death and post-mortem data management. While cultural factors were scoped out in this thesis, questions about their influence emerged during the comparison of the GDPR and China's PIPL. As cultures differ in how they approach death, grief, and legacy, further research could support the development of more culturally sensitive tools and legal frameworks for managing digital legacies.

Bibliography

- [1] *About inactive account deletion*. Accessed: 16-03-2025. URL: <https://faq.whatsapp.com/828406668498455/?helpref=search&query=inactivity>.
- [2] *About the Learning Phase*. Accessed: 18-03-2025. URL: <https://www.facebook.com/business/help/112167992830700?id=561906377587030>.
- [3] *Accessing Outlook.com, OneDrive and other Microsoft services when someone has died*. Accessed: 18-03-2025. URL: <https://support.microsoft.com/en-us/account-billing/accessing-outlook-com-onedrive-and-other-microsoft-services-when-someone-has-died-ebbd2860-917e-4b39-9913-212362da6b2f>.
- [4] Akmaljon Akramov et al. "The Impact of Digitalization in Inheritance Law". In: *Qubahan Academic Journal* 4 (Aug. 2024), pp. 100–134. DOI: 10.48161/qaj.v4n3a863.
- [5] BestVPN.org. *Internet Privacy Index*. Accessed: 28-03-2025. 2024. URL: <https://bestvpn.org/privacy-index/>.
- [6] Buffer. *20+ Top Social Media Platforms to Grow Your Brand in 2025*. Accessed: 15-03-2025. 2025. URL: <https://buffer.com/resources/social-media-platforms/>.
- [7] *Claim a decedent's Coinbase account*. Accessed: 13-03-2025. URL: <https://help.coinbase.com/en/coinbase/managing-my-account/other/how-do-i-gain-access-to-a-deceased-family-members-coinbase-account>.
- [8] Clocr. *Clocr: Estate Planning | Online Will | Executor | Digital Legacy*. Accessed: 16-03-2025. 2023. URL: <https://clocr.com/>.
- [9] *Contacting X about a deceased family member's account*. Accessed: 19-03-2025. URL: <https://help.x.com/en/rules-and-policies/contact-x-about-a-deceased-family-members-account>.
- [10] *Create a memory profile or close the account if a member has passed away*. Accessed: 20-03-2025. URL: <https://www.linkedin.com/help/linkedin/answer/a1336663/>.
- [11] Crypto.com. *Global Cryptocurrency Owners Grow to 659 Million Through 2024*. Accessed: 16-03-2025. Feb. 2025. URL: <https://crypto.com/en/company-news/global-cryptocurrency-owners-grow-to-659-million-through-2024>.
- [12] *Data Inheritance: How It Works and Why It Matters*. Accessed: 16-03-2025. URL: <https://help.securesafe.com/data-inheritance>.

- [13] Datatilsynet. *Arbeidsgivers behandling av personopplysninger ved arbeidstakers død*. Accessed: 04-03-2025. 2024. URL: <https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/arbeidsgivers-behandling-av-personopplysninger-ved-arbeidstakers-dod/>.
- [14] Datatilsynet. *Arbeidsgivers behandling av personopplysninger ved arbeidstakers død*. Accessed: 08-03-2025. 2024. URL: <https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/arbeidsgivers-behandling-av-personopplysninger-ved-arbeidstakers-dod/?print=true>.
- [15] *Deceased LinkedIn member*. Accessed: 22-03-2025. URL: <https://www.linkedin.com/help/linkedin/answer/a1380121>.
- [16] *Deceased or Incapacitated Users*. Accessed: 16-03-2025. URL: <https://support.discord.com/hc/en-us/articles/19872987802263--Deceased-or-Incapacitated-Users>.
- [17] *Delete Account*. Accessed: 16-03-2025. URL: <https://support.signal.org/hc/en-us/articles/360007061192-Delete-Account>.
- [18] DeleteMe. *DeleteMe – Secure Your Information And Privacy*. Accessed: 16-03-2025. 2025. URL: <https://www.deleteme.com/>.
- [19] Digitaliserings- og Ligestillingsministeriet. *Digitaliserings- og Ligestillingsministeriet*. Accessed: 2025-05-19. 2024. URL: <https://www.digmin.dk/>.
- [20] Digitaliseringsstyrelsen. *eIDAS2 og den digitale identitetstegnebog*. Accessed: 09-03-2025. 2025. URL: <https://digst.dk/it-loesninger/eid-og-single-digital-gateway/eidas2-og-den-digitale-identitetstegnebog/>.
- [21] DLA Piper. *Data Protection Laws of the World*. Accessed: 15-03-2025. 2024. URL: <https://www.dlapiperdataprotection.com/>.
- [22] e-Boks A/S. *e-Boks Private Platform*. Accessed: 28-04-2025. 2025. URL: <https://private.e-boks.com/>.
- [23] *Emergency Access | Bitwarden*. Accessed: 16-03-2025. URL: <https://bitwarden.com/help/emergency-access>.
- [24] European Commission. *Digital Economy and Society Index (DESI)*. Accessed: 22-03-2025. 2025. URL: <https://digital-strategy.ec.europa.eu/en/policies/desi>.
- [25] European Commission. *eIDAS Regulation and European Digital Identity*. European Digital Strategy, European Commission. Accessed: 16-04-2025. 2024. URL: <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>.
- [26] European Commission. *EU Digital Identity Wallet Home*. Accessed: 09-03-2025. 2025. URL: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET-EU+Digital+Identity+Wallet+Home>.
- [27] European Commission. *The Digital Markets Act: ensuring fair and open digital markets*. European Commission policy overview. Accessed: 16-04-2025. 2023. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (visited on 05/19/2025).

- [28] European Commission. *The Digital Services Act: ensuring a safe and accountable on-line environment*. European Commission digital policy page. 2023. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.
- [29] European Law Institute. *ELI Adopts a New Project on Succession of Digital Assets, Data and Other Digital Remains*. European Law Institute announcement. Accessed: 16-04-2025. 2024. URL: <https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-adopts-a-new-project-on-succession-of-digital-assets-data-and-other-digital-remains/>.
- [30] European Parliament. *EU Digital Markets Act and Digital Services Act explained*. Accessed via European Parliament official site. Accessed: 16-04-2025. 2021. URL: <https://www.europarl.europa.eu/topics/en/article/20211209ST019124/eu-digital-markets-act-and-digital-services-act-explained>.
- [31] Fillout.com. *Fillout: Forms that do it all*. Accessed: 20-02-2025. 2023. URL: <https://www.fillout.com>.
- [32] Final Security. *Final Security – Digital Legacy & Estate Platform*. Accessed: 16-03-2025. 2025. URL: <https://finalsecurity.co/>.
- [33] *Folkbokföringslag (1991:481)*. Accessed: 19-05-2025. 1991. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/folkbokforingslag-1991481_sfs-1991-481/.
- [34] GDPR-Info.eu. *General Data Protection Regulation (GDPR) – Official Legal Text*. Accessed 28-03-2025. 2024. URL: <https://gdpr-info.eu/>.
- [35] *GDPR Recital 27 – Personal Data of Deceased Persons*. Accessed: 03-03-2025. 2016. URL: <https://gdpr-info.eu/recitals/no-27/>.
- [36] Google. *Colaboratory*. Accessed: 28-03-2025. 2024. URL: <https://colab.research.google.com/>.
- [37] Carsten Grimm and Sonia Chiasson. "Survey on the Fate of Digital Footprints after Death". In: Jan. 2014. DOI: 10.14722/usec.2014.23049.
- [38] Jack Holt, James Nicholson, and Jan David Smeddinck. "From Personal Data to Digital Legacy: Exploring Conflicts in the Sharing, Security and Privacy of Post-mortem Data". In: *Proceedings of the Web Conference 2021*. Accessed: 05-03-2025. ACM, 2021. DOI: 10.1145/3442381.3450030. URL: <https://dl.acm.org/doi/pdf/10.1145/3442381.3450030>.
- [39] *How do I delete my account?* Accessed: 18-03-2025. URL: <https://support.reddithelp.com/hc/en-us/articles/204579509-How-do-I-delete-my-account>.
- [40] *How to cancel an account for a deceased Netflix member*. Accessed: 16-03-2025. URL: <https://help.netflix.com/en/node/110165>.
- [41] *How To Delete A Loved One's TikTok Account | GoodTrust*. Accessed: 18-03-2025. URL: <https://mygoodtrust.com/articles/how-to-delete-a-loved-ones-tiktok-account>.

- [42] *How to request access to a deceased family member's Apple Account*. Accessed: 17-03-2025. URL: <https://support.apple.com/en-us/102431>.
- [43] *I'd like to report an account of a person who passed away*. Accessed: 18-03-2025. URL: <https://help.snapchat.com/hc/en-us/articles/27504454933908-I-d-like-to-report-an-account-of-a-person-who-passed-away>.
- [44] Forum of Incident Response and Security Teams (FIRST). *Common Vulnerability Scoring System v4.0: Specification Document*. Accessed: 02-04-2025. 2023. URL: [url{https://www.first.org/cvss/specification-document}](https://www.first.org/cvss/specification-document).
- [45] Inheriti. *Inheriti® – Secure Your Digital Life*. Accessed: 16-03-2025. 2025. URL: <https://inheriti.com/>.
- [46] European Law Institute. *ELI Principles on the Use of Digital Assets as Security*. SSRN Working Paper. Accessed: 16-04-2025. 2023. URL: <https://ssrn.com/abstract=4318347>.
- [47] Integritetsskyddsmyndigheten. *Vad är personuppgifter?* Accessed: 19-03-2025. 2021. URL: <https://www.imy.se/privatperson/dataskydd/introduktion-till-gdpr/vad-ar-personuppgifter/>.
- [48] Mark Jia. "Authoritarian Privacy". In: *University of Chicago Law Review* 91 (2024). Georgetown University Law Center Research Paper No. Forthcoming. doi: 10.2139/ssrn.4362527. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4362527.
- [49] Justitsministeriet. *Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (Databeskyttelsesloven)*. Senest opdateret version fra Retsinformation. Accessed: 20-05-2025. 2025. URL: <https://www.retsinformation.dk/eli/lta/2018/502>.
- [50] R. Kaushal et al. *Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database*. arXiv preprint arXiv:2404.02894. Accessed: 19-05-2025. 2024. URL: <https://arxiv.org/abs/2404.02894>.
- [51] Jette Kofoed and Malene Larsen. "A snap of intimacy: Photo-sharing practices among young people on social media". In: *First Monday* 21 (Oct. 2016). doi: 10.5210/fm.v21i11.6905.
- [52] Cristiano Maciel and Vinicius Pereira. "Post-mortem Digital Legacy: Possibilities in HCI". In: Aug. 2015, pp. 339–349. ISBN: 978-3-319-21005-6. doi: 10.1007/978-3-319-21006-3_33.
- [53] Cristiano Maciel et al. "Defining Digital Legacy Management Systems' Requirements". In: *Enterprise Information Systems. ICEIS 2021. Lecture Notes in Business Information Processing*. Ed. by Joaquim Filipe et al. Vol. 455. Springer, Cham, 2022, pp. 256–279. URL: https://link.springer.com/chapter/10.1007/978-3-031-08965-7_17.
- [54] Meta Platforms, Inc. *About Meta*. Accessed: 23-03-2025. 2025. URL: <https://about.meta.com/>.

- [55] Ministry of Justice and Public Security. *Act relating to the processing of personal data (The Personal Data Act)*. Accessed: 04-03-2025. 2018. URL: <https://lovdata.no/dokument/NLE/lov/2018-06-15-38>.
- [56] Miro. *Miro*. Accessed: 02-03-2025. 2024. URL: <https://miro.com/da/>.
- [57] MitID. *MitID - Din digitale identitet*. Accessed: 2025-05-19. 2024. URL: <https://www.mitid.dk/>.
- [58] My-Legacy.ai. *My-Legacy.ai – AI-Powered Estate Planning*. Accessed: 16-03-2025. 2025. URL: <https://my-legacy.ai/>.
- [59] *New NordPass Feature Is Here — Emergency Access*. Accessed: 16-03-2025. URL: <https://nordpass.com/blog/introducing-emergency-access/>.
- [60] TV 2 Nyheder. *Deres far døde i udlandet – 15 måneder senere er han stadig ikke erklæret død*. Accessed: 10-04-2025. 2025. URL: <https://nyheder.tv2.dk/samfund/2025-04-22-deres-far-doede-i-udlandet-15-maaneder-senere-er-han-stadig-ikke-erklaret-doeed>.
- [61] Carl Öhman and Luciano Floridi. “An ethical framework for the governance of the digital afterlife”. In: *Nature Human Behaviour* 2.11 (2018), pp. 808–810.
- [62] *PIPL Article 49 – Rights in Relation to Deceased Individuals*. Accessed March 2025. 2021. URL: <https://personalinformationprotectionlaw.com/PIPL/article-49/>.
- [63] *PIPL Information. Personal Information Protection Law (PIPL) – Unofficial English Translation*. Accessed: 12-03-2025. 2024. URL: <https://personalinformationprotectionlaw.com/>.
- [64] *Privacy Policy Agreement*. Accessed: 16-03-2025. URL: https://store.steampowered.com/privacy_agreement/.
- [65] PrivacyHQ. *World Data Privacy Rankings by Country*. Accessed: 15-03-2025. 2024. URL: <https://privacyhq.com/news/world-data-privacy-rankings-countries/>.
- [66] ProductPlan Editorial Team. *MoSCoW Prioritization*. Accessed: 08-03-2025. n.d. URL: <https://www.productplan.com/glossary/moscow-prioritization/>.
- [67] *Report a deceased person’s account on Instagram*. Accessed: 19-03-2025. URL: <https://help.instagram.com/264154560391256>.
- [68] *Request to close a deceased member’s LinkedIn profile*. Accessed: 19-03-2025. URL: <https://www.linkedin.com/help/linkedin/ask/ts-rmdmlp>.
- [69] *Request to Memorialize or Remove an Account*. Accessed: 18-03-2025. URL: <https://www.facebook.com/help/1111566045566400/>.
- [70] Simplicity Cremations. *Dealing with social media accounts after death*. Accessed: 02-03-2025. 2024. URL: <https://www.simplicity.co.uk/advice/dealing-with-social-media-accounts-after-death>.
- [71] *Skattedatalagen (SdbL) – Tax Data Act*. Accessed: 17-05-2025. 2011. URL: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/skattedatalag-2011-1244_sfs-2011-1244.

- [72] Skatteverket. *Vad är personuppgifter och behandling av personuppgifter? Rättslig vägledning*, Skatteverket. Accessed: 04-03-2025. 2025. URL: <https://www4.skatteverket.se/rattsligvagledning/edition/2025.2/379273.html>.
- [73] *Steam Subscriber Agreement*. Accessed: 15-03-2025. URL: https://store.steampowered.com/subscriber_agreement/.
- [74] *Steam Support :: Account Deletion - Common Questions*. Accessed: 16-03-2025. URL: <https://help.steampowered.com/en/faqs/view/21A6-7C93-6CFE-100B>.
- [75] *Steam Support :: Providing Proof of Ownership*. Accessed: 16-03-2025. URL: <https://help.steampowered.com/en/faqs/view/40A0-8B4B-B54B-C51A>.
- [76] H Strack et al. "eID & eIDAS at University Management-Chances and Changes for Security & legally Binding in cross boarder Digitalization". In: *Proceedings of the EU-NIS 23rd Annual Congress, Münster, Germany*. 2017, pp. 7–9.
- [77] *Submit a request regarding a deceased user's account*. Accessed: 16-03-2025. URL: <https://support.google.com/accounts/troubleshooter/6357590>.
- [78] *The complete guide to digital estate planning | 1Password*. Accessed: 18-03-2025. URL: <https://blog.1password.com/get-started-digital-estate-planning/>.
- [79] The Norwegian Data Protection Authority. *Norway's Personal Data Act (Personopplysningsloven)*. Accessed: 19-03-2025. 2024. URL: <https://www.datatilsynet.no/en/regulations-and-tools/regulations/>.
- [80] European Union. *Regulation (EU) No 910/2014 (eIDAS Regulation)*. Accessed: 20-04-2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.
- [81] UpGuard. *How to Assess Cyber Risk for Potential Vendors (Complete Guide)*. Accessed: 02-04-2025. 2024. URL: <https://www.upguard.com/blog/how-to-assess-cyber-risk-for-potential-vendors>.
- [82] Vault12. *Vault12 – Crypto Inheritance & Backup*. Accessed: 16-03-2025. 2025. URL: <https://vault12.com/>.
- [83] Monica Whitty et al. "Individual differences in cyber security behaviors: an examination of who is sharing passwords". In: *Cyberpsychol Behav Soc Netw* 18.1 (2015), pp. 3–7.

Appendix A: Qualitative interview questions

This appendix includes the semi-structured interview guide and an overview of the five qualitative interviews conducted as part of the thesis research.

Questions for interview: Close family member to deceased relative

Note: Interviewee responded on the quantitative survey. The following questions take basis in their survey submission.

1. In the survey, you mentioned that MitID was deactivated very quickly after the death — could you elaborate on how that happened?
2. What kind of information or services did you try to access via MitID?
3. What steps did you take to gain access?
4. What responses or feedback did you receive from authorities or systems when you attempted to gain access?
5. What did you experience as the main obstacles in the process?
6. How did it affect you personally or emotionally to be in that situation?
7. If it were up to you, how would you have wanted the process to unfold?
8. How do you envision an ideal solution — for example, shared access, digital wills, or automatic transfer?
9. Has this experience made you think about what should happen to your own digital data?
10. Have you taken any steps since then to secure your own data?
11. In your opinion, how can we improve the way we talk about digital death and digital legacies?

12. How would you feel about using a national solution or portal for digital inheritance?
13. What requirements would you, as a citizen, expect from such a solution before you would use it?
14. Should it be the individual who decides what access should be granted — or the heirs?
15. What do you think about the idea of creating a digital will directly through MitID?
16. Have you spoken with others who have had similar experiences?
17. Do you have any advice for others who might find themselves in a similar situation?

Questions for interview: Family member (death abroad)

Background

1. Could you briefly describe how you first became aware of the challenges related to getting the death officially recognised in Denmark?
2. Which Danish authorities have you been in contact with during the process?

Data Handling Issues

3. What specific problems have you encountered regarding the handling of your father's data (e.g., bank, hospital, social media)?
4. Have you tried contacting private companies (such as a bank or social media platforms) directly to get help?
 - (a) If yes — how did they respond?

Privacy and Dignity

5. Do you feel that your father's privacy is being respected, given the current situation?
6. How does it make you feel to continue receiving messages or mail addressed to your father, when his death is not officially recognised?

Legal and Bureaucratic Challenges

7. What is your experience of how the law currently handles situations like yours?
 - (a) What changes in legislation or administrative practices might have made a difference in your case?

Broader Reflections

8. What advice would you give to others who may face a similar situation?

9. How do you think we could better ensure respect for the data and dignity of deceased individuals in future cases?
10. How has this situation affected your own thoughts about managing your digital data?

Questions for interview: Chief Information Security Officer (CISO) Head of IT Support

1. Standard procedures

1. Can you describe the general process followed at SDU when an employee passes away, especially in relation to email, OneDrive, and IT equipment?
2. Is this process documented formally, or handled case-by-case?
3. How does this compare to a regular employee offboarding (e.g., resignation or retirement)?
4. Is there currently a defined grace period before accounts and data are deleted?

2. Access requests from next of kin

5. What types of requests do you typically receive from relatives of the deceased?
6. Under what conditions can access be granted to emails or files in OneDrive?
7. How is access approved, and who makes the final decision?
8. Have there been situations where entire mailboxes were requested? How was that handled?
9. How is sensitive data handled to avoid emotional or ethical breaches during this process?

3. System and security concerns

10. What happens when another platform is tied to the SDU email of the deceased? How is access managed?
11. Are there risks associated with employees using institutional emails to register private services?
12. What challenges exist around shared documents or links in OneDrive that remain accessible posthumously?
13. How does your team ensure compliance with security protocols while being respectful to grieving families?

4. Legal, ethical and organisational boundaries

14. Are current processes based on specific legal frameworks or internal SDU policy?
15. What are the limitations you face legally or ethically when dealing with post-mortem data?
16. Do you believe existing Danish law adequately supports institutions in managing employee data after death?
17. How do you strike a balance between respecting privacy and ensuring operational continuity?

5. Future needs and reflections

18. In your opinion, what would an ideal solution look like for handling digital remains of employees?
19. Are there any internal changes SDU is planning (e.g., new policies for private use of work accounts)?
20. What recommendations would you make to other institutions facing similar challenges?
21. Do you see any areas where SDU could improve its handling of digital legacies?

Questions for interview: Astrid Waagstein, PhD in post-mortem data rights**1. Background and motivation**

1. Could you start by telling us about your research in data rights and what led you to focus on post-mortem data?

2. Access rights and ethical boundaries

2. In your view, who should have the right to access personal digital data such as emails, photos, or social media accounts after a person's death?
3. What ethical tensions arise when trying to balance the privacy of the deceased with the needs of their surviving relatives?
4. What might a more ethically sound or structured model of post-mortem access look like?

3. Granular access and data types

5. What are the challenges associated with current models of access, where it is often either fully denied or fully granted?

6. How could digital data be classified or tiered to allow more nuanced access rights?

4. AI and posthumous identity

7. What are the ethical implications of using personal data from deceased individuals in AI training or generative models?
8. Could large-scale AI systems alter or distort someone's legacy or identity after death?
9. Do you think there is a need for specific legal or consent-based protections in this area?

Questions for interview: Privacy engineering lecturer

1. Data classification and privacy types

1. In your view, how should we distinguish between different types of personal data when considering digital legacy (e.g., private messages vs. professional documents)?
2. Are there types of privacy that become less relevant or more important after death?

2. Data donation and ownership

3. What are your thoughts on people donating their digital data (e.g., social media, documents) after death — is it technically or ethically feasible?
4. Should there be technical limitations on what types of data can be shared posthumously?

3. Risks and reflections

5. Are technical risks like inference attacks something institutions should worry about when handling data from deceased users?
6. From your perspective, what is one important thing students or developers should keep in mind when building systems that deal with post-mortem data?

4. Comparative legal perspectives

7. Are you aware of any legal frameworks outside the EU that offer interesting approaches to personal data after death, or that differ significantly from the GDPR in this area?

Appendix B: Unified Post-Mortem Protocol Exploration Miro Board

UPAP

Solution: Unified Post-Mortem Access Protocol (UPAP)

A standard for service providers

Plan

1. Problem Definition & Scope

- a. What gaps exist in current system?
- b. Which digital assets will the protocol cover?
- c. How will the protocol handle jurisdictional conflicts? (e.g. cross-border laws)

2. Core Principles & Compliance

- a. What legal frameworks must the protocol align with?
- b. How will privacy for the deceased be balanced with next-of-kin access?
- c. Will the protocol enforce data transfer or deletion by default?

3. Technical Architecture

- a. How will death events be verified?
- b. What authentication mechanisms will next-of-kin use?
- c. How will the protocol integrate with existing platforms?

4. User Workflow & Features

- a. How will users designate next-of-kin?
- b. What metadata must accompany digital assets?
- c. How will the protocol notify stakeholders?
 - i. How do we avoid fake death certificate?
- d. What features will be proposed?
 - i. Death verification
 - ii. Next-of-kin access

5. Stakeholder Coordination

- a. How will service providers opt in?
- b. What resources does it require from the service provider?
- c. What role will governments play?

6. Validation & Testing (PoC)

- a. What metrics will validate success?
- b. How will ethical risks be mitigated?

1. Problem Definition & Scope

Gaps in current systems

1. 50% of SPs does not handle post-mortem data management
2. No laws explicitly stating how SPs should handling post-mortem data
3. Limited pre-planning tools
4. No granular asset selection
5. Opaque policies, buried in terms of services
6. Password dependent sharing with next-of-kin
7. No standard death verification, inconsistent triggers
8. Profit-driven data retention?
9. No legal obligation for SP to setup DLMS
10. Inconsistent inactivity policies
11. User unpreparedness
12. Inconsistent handling format

Digital Assets covered by protocol

1. Social Media account
 - a. e.g. Facebook, Instagram, LinkedIn etc
2. Messing platforms
 - a. WhatsApp, Messenger, Signal
3. Email accounts
 - a. Gmail, Outlook
4. Content and Media
 - a. Google Drive, Dropbox
5. Entertainment
 - a. Spotify, Netflix
 - b. Steam
6. Password managers
7. Intellectual Property & Online business
 - a. Hosting providers

Handling jurisdictional conflicts

The UPAP will follow a tiered handling of legal conflicts:

1. User's own will and instructions
2. User's home country laws
 - a. User can choose on sign-up
3. Service Providers policy
 - a. If they don't conflict
4. Use international agreements where possible
 - a. E.g GDPR in Europe if applicable
5. Disagreement resolution
 - a. Individual handling (case-by-case approach like SDU)

Centralised vs Decentralised

Selected solution

| Category | Centralised (Third-party) | Decentralised |
|--------------------|--|--|
| Security | Pros <ul style="list-style-type: none"> Quality control on all SPs Can be in Europe without SPs being in Europe and therefore adhering to legal frameworks Cons <ul style="list-style-type: none"> Single point-of-failure e.g. supply-chain risk All SPs bottleneck at the third parties security | Pros <ul style="list-style-type: none"> Direct control over data access and encryption Each SPs is a point-of-failure, no single point-of-failure Cons <ul style="list-style-type: none"> High in-house cost for security tooling and audits SPs legal obligations might conflicts users legal coverage in their respective country |
| Compliance | Pros <ul style="list-style-type: none"> Only have to vet one entity for compliance check Cons <ul style="list-style-type: none"> Trust might be affected Third-party might be lobbied by the bigger SPs (bias) | Pros <ul style="list-style-type: none"> Trust is defaulted to the users existing level of trust No bias from external entities Cons <ul style="list-style-type: none"> Resource-intensive legal adhering for platforms operating in multiple countries |
| User Experience | Pros <ul style="list-style-type: none"> User has 1 unified dashboard for connecting accounts Next-of-kin will only have to interact with 1 entity Cons <ul style="list-style-type: none"> Huge overhead in integrating with all kind of service providers | Pros <ul style="list-style-type: none"> Native integration with existing DLMS solutions in SPs Higher level of customisation for post-mortem data management Cons <ul style="list-style-type: none"> User has to set it up for each SP Next-of-kin have to prove death and ownership with each SP SP can have different requirements for death verification |
| Cost Efficiency | Pros <ul style="list-style-type: none"> Shared compliance burden (e.g. EU has a shared solution) Cons <ul style="list-style-type: none"> Alignment between participating member states Unclear definition of Non-EU members | Pros <ul style="list-style-type: none"> Avoid any fee towards third-party Cons <ul style="list-style-type: none"> Higher initial development investment |
| Death Verification | Pros <ul style="list-style-type: none"> National identity systems can be used One death verification can be used for all SPs Cons <ul style="list-style-type: none"> Tremendous effect in case of a false positive | Pros <ul style="list-style-type: none"> SP can use internal activity to determine death Each platform depending on the value of the assets can set higher/lower requirements for the death verification Cons <ul style="list-style-type: none"> Platform-specific false-positive risks |

2. Core Principales & Compliance

Legal Frameworks

1. Inspired by GDPR
 - a. Service Provider should handle data of living individuals in records of a deceased individual
2. Opt-in for 10+ years of GDPR-like protection extension
3. Opt-out of auto-deletion and move to that next of kin inherits data rights like in China

Privacy & Access balance

1. Balancing personal preference of the user with what their wishes are in contrast with the laws.
2. User should be able to choose what the next of kin has access to
3. User should be able to choose what the next of kin can do with the data; edit, delete, transfer etc
4. Option of storing data for future research if wanted (like organ donation)

Default handling

1. Deletion by default
2. Unless a plan is set up
 - a. E.g. user has delegated access to next of kin
3. Data will by default be hidden on the service providers site, the data will still be available for the next of kin within a grace period
 - a. 6-24 months
 - i. Balance between costs of storing data
 - ii. Grieving period
 - iii. Based on SDU and Service Provider

3. Technical Architecture

How will death events be verified?

How it is handled today

One or more of these is used to verify death:

1. **Death certificate**
2. **Proof of relationship** (e.g., marriage certificate, birth certificate, will, estate letter, power of attorney)
3. **Probate certificate / court order / letter of administration**
4. **Valid photo ID of requester** (passport, driver's license, etc.)
5. **Account details** (email address, username, profile URL)
6. **Obituary or memorial card**
7. **Billing or payment information**
8. **Legal proof of authority** (executor/administrator documentation)

How UPAP handled death events

User has set-up an emergency contact before their death. Emergency contact will be notified throughout the entire process.

Process

1. Requester initiates death verification
 - a. See severity table for what is required
2. Deceased user and emergency contact receives notification about request
 - a. The process can be stopped here
3. After X days the user receives an email
 - a. The user's activity logs are also monitored to see any proof of life
 - i. Activity log should be relative to the average usage of accounts
4. After X days the user receives an SMS
5. After X days the user receives a phone call
6. If the process has not been stopped, the user will be deemed digitally dead

3. Technical Architecture

| Severity Level | Category | Example Service Providers | Rationale (Data Volume, Sensitivity, Harm Potential) | |
|----------------|--------------------------------|--------------------------------|--|--|
| Critical | Password Managers | LastPass, 1Password, Bitwarden | Store all user credentials; breach exposes entire digital identity and financial access. | |
| Critical | Email Accounts | Gmail, Outlook | Central hub for identity, password resets, sensitive communications, and access to other services. | |
| High | Content & Media Storage | Google Drive, Dropbox | Store personal, business, and legal documents; often includes sensitive files and backups. | |
| High | Intellectual Property/Hosting | GoDaddy, Bluehost, AWS, GitHub | Host business-critical data, websites, and intellectual property; breach can destroy businesses or leak proprietary assets. | |
| High | Messaging Platforms | WhatsApp, Messenger, Signal | Sensitive conversations and contacts; WhatsApp collects significant metadata, Signal less so. | |
| High | Social Media | Facebook, Instagram, LinkedIn | Large amount of personal data, social graphs, and reputation at risk; can be used for impersonation, fraud, or social engineering. | |
| Medium | Steam (Gaming + Market) | Steam | Stores payment info, game licenses, and valuable digital assets (marketplace items); breach can result in financial and identity loss. | |
| Low | Entertainment | Spotify, Netflix | Personal preferences, some payment info, but generally lower direct harm if breached. | |
| Low | Other Streaming/Minor Accounts | Pandora, Hulu, minor forums | Minimal sensitive data, limited impact if breached. | |

| Severity Level | Definition | Verification Requirements | Process levels | |
|----------------|--|---|----------------------------------|--|
| All | Verification requirements for all severity levels | Official death certificate Valid photo ID of requester Account details Proof of relationship | Mail + SMS + Call + Activity log | |
| Critical | Accounts/services that, if compromised, could result in catastrophic harm (e.g., full identity theft, total financial loss, or destruction/exposure of highly sensitive data). | Preassigned emergency contact | Mail + SMS + Call + Activity log | |
| High | Accounts with significant sensitive data or control over other important services. Compromise could lead to major financial, legal, or reputational harm. | Preassigned emergency contact | Mail + SMS + Call + Activity log | |
| Medium | Accounts with moderate personal or social data. Compromise could cause inconvenience, impersonation, or moderate harm, but not catastrophic loss. | No additional requirements | Mail + SMS + Activity log | |
| Low | Accounts with minimal sensitive data and limited impact if compromised. | No additional requirements | Mail verification + Activity log | |

3. Technical Architecture

NOK Authentication mechanisms

1. User assign 1 or more emergency contacts on sign-up
 - a. For existing users they should be prompted with a option to set their post-mortem management preferences
2. Valid photo ID of requester

Integration to Service Providers

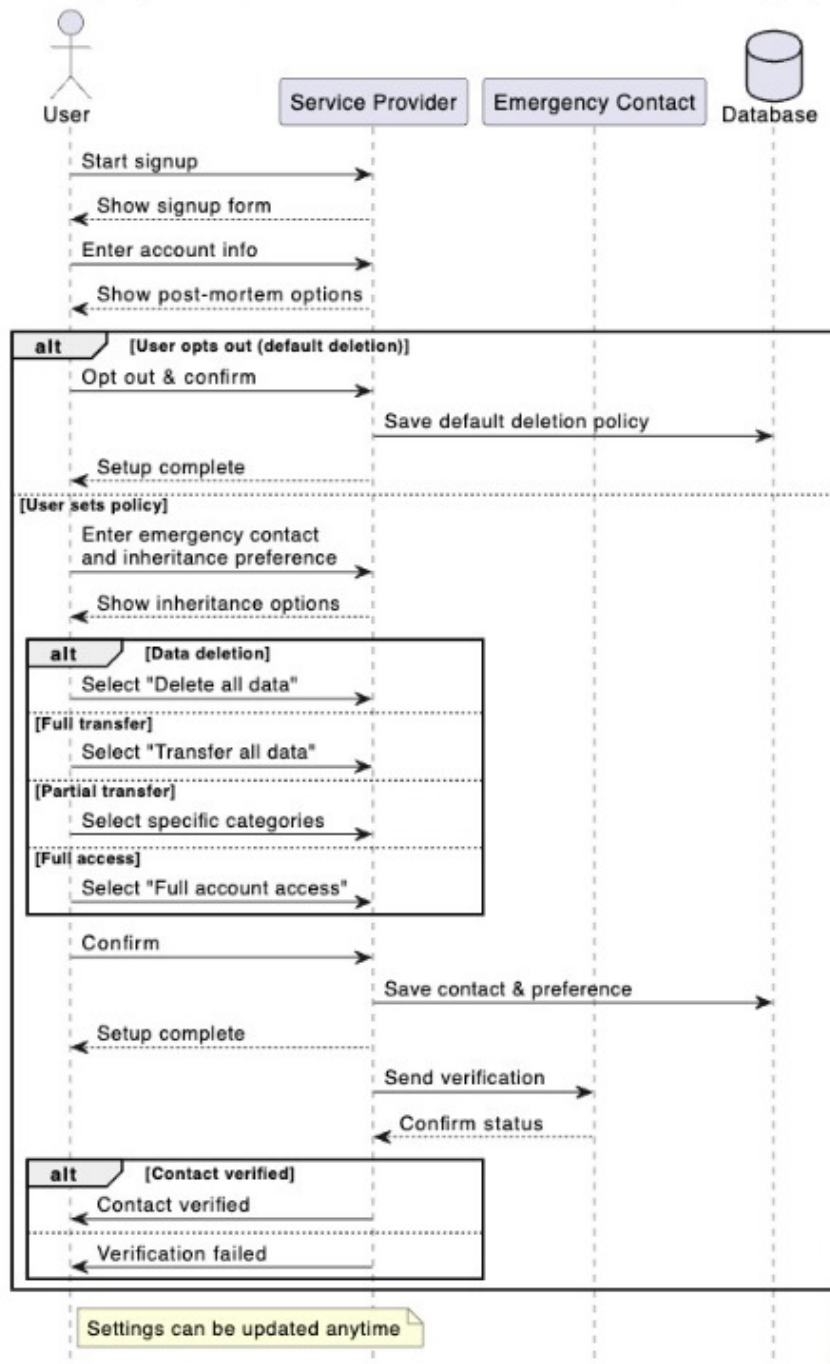
1. **User creation extension**
 - a. Possibility to assign emergency contact
 - i. *Emergency contacts can be assigned a role for different preferences*
 - b. Set preferences for what happens upon death
 - i. Full access
 - ii. Transfer of all data
 - iii. Transfer of selected data
 1. Private/Public when applicable
 - iv. Deletion (default)
2. **User update feature**
 - a. For existing users
 - i. Get a notification that they have to set their preferences
 - b. Or if users wants to change emergency contact or preferences
3. **Death Verification flow**
 - a. Ability for NOK to submit a death event
 - i. Document submission
 - b. Handling of submissions
 - c. Technical implementation for heart beat events
4. **Handling when a death is verified**
 - a. Look at users preferences or default to deletion

As a starting point, Proof of relation is a familial relation. In some cases, it can be extended to a friend or employer/colleague.

4. User Workflow & Features

How will users designate next-of-kin?

Emergency Contact & Post-Mortem Data Preferences during User Signup



Remember to point out that existing users will experience a similar flow the first time they log in after UPAP is implemented.

4. User Workflow & Features

What metadata must accompany digital assets?

1. User should be able to flag data in 2 or more categories in order to choose what the emergency contact will receive or have access to

The service provider should implement the meta data so it fits the nature of their service, as we cant make a one size fits all

Examples

- High level: A account provider should give the user the ability to share Google Drive but not Google Mail
- Low level: In Google Drive a user can set a flag on each folder fx. PRIVATE

How do we avoid fake death certificate?

- For the UPAP MVP the death certificates will not be validated but the heart beat process will serve as a multi-factor verification

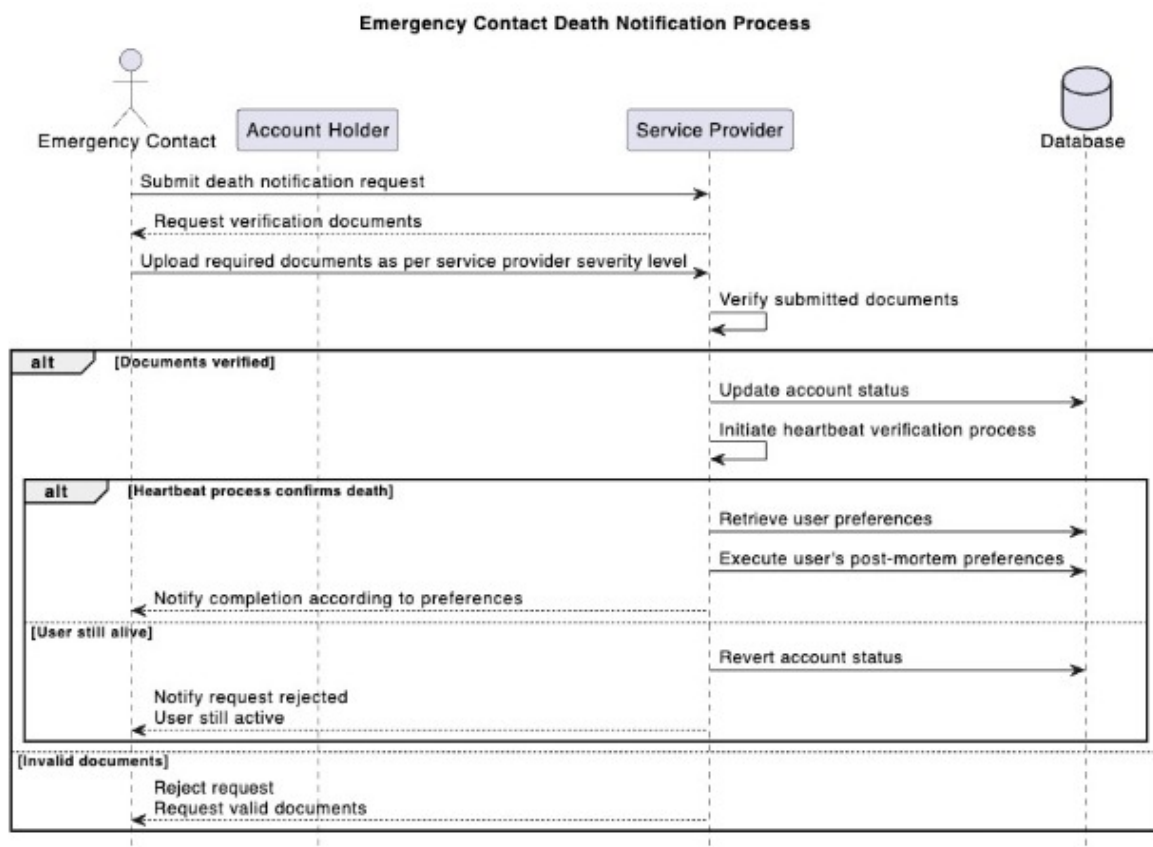
This can be implemented in future works, but have to integrated with all nations where the Service Provider operates or use eIDAS if they can unify the verification processes for Europe.

4. User Workflow & Features

How will the protocol notify stakeholders?

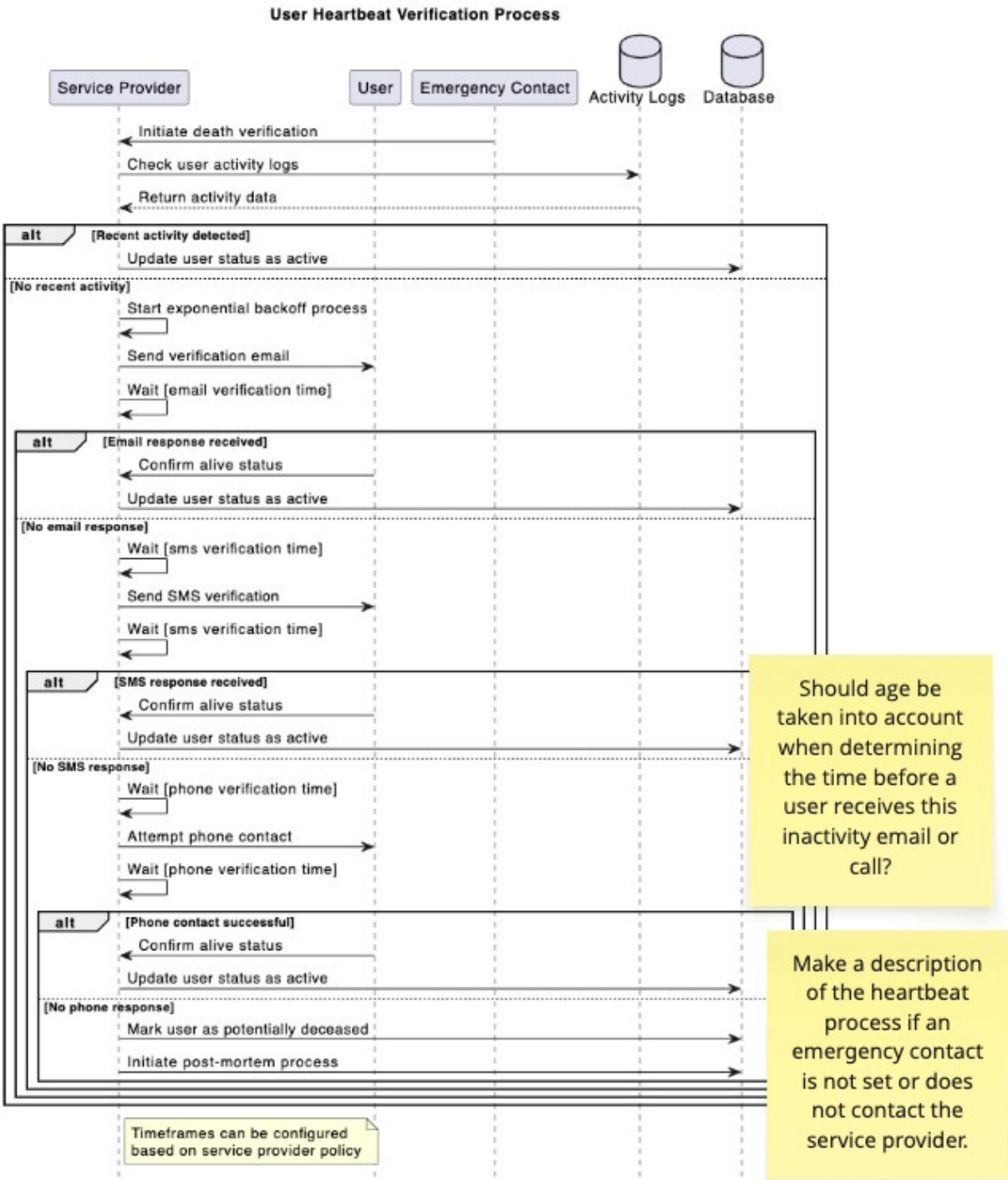
- User
 - Alive: In-platform, mail, sms (dependent on platform)
 - During death verification: Notification, mail, sms, phone call
 - Deceased: N/A
- Emergency contact
 - Before user is deceased: Mail
 - After user is deceased: Platform-specific request form, mail

How will the protocol notify stakeholders?



4. User Workflow & Features

Heartbeat Process



4. User Workflow & Features

Inactivity deactivation

- If no emergency contact
- Use standard inactivity deactivation as seen today in Service Providers
- 6 - 24 months

Future Explorations

Digital Death Certificates:
Replace physical documentation with eIDAS 2.0-validated digital certificates, auto-verifiable via national registries (e.g., Denmark's CPR system) [Legal Framework Analysis].

Pre-Mortem Delegation Tools: Require platforms to integrate features like:

Legacy contacts (Facebook, Apple)

Emergency access (1Password, SecureSafe)

Automated data transfers (Google's Inactive Account Manager)

EU-wide regulation mandating UPAP compliance for all providers operating in the EU.

Hvad gør vi hvis en hacker er involveret eller data er outdated?

Grace Periods: Mandate a 6-month minimum before account deletion (aligning with SDU's proposed policy) to prevent data loss (e.g., MitID's abrupt closure blocked health records)

5. Stakeholder Coordination

How will service providers opt in?

- In order for UPAP to be implemented by SPs, there should be one of more reasons:
 - Enhance trust with users
 - Forced by legal frameworks (not available today)
 - Clear policies for handling data

Legal

- Providers can add UPAP requirements into their service agreements or terms of service, making the commitment legally binding
- UPAP will only become mandatory if backed by law.
 - With fines as GDPR did
- **Government Mandate**
 - If UPAP becomes law (for example, via EU regulation), all service providers operating in the EU would be required to comply, similar to how GDPR and NIS 2 work.

Ethical

- Respecting User Autonomy and Wishes
- Supporting Emotional Well-being of Families

Technical

- Providers implement the technical features required by UPAP, such as:
 - Letting users assign emergency contacts
 - Setting post-mortem preferences
 - Handling death verification and next-of-kin authentication
- Existing users would be prompted to set their preferences the next time they log in after UPAP is rolled out.

Certification or Auditing

- Providers could go through a certification process or an audit to show they meet UPAP requirements.
- This could be used for marketing or to build trust with users and partners.

5. Stakeholder Coordination

What resources does it require from the service provider?

- **Technical Development**
 - Options for users to assign emergency contact and set post-mortem data preferences
 - Build or adapt interfaces for next-of-kin to request access or deletion after a user's death.
 - Implement metadata tagging so users can flag which data/assets should be accessible, deleted, or kept private after death.
 - Integrate systems to verify death events (internal "heartbeat" checks using user activity).
- **Security and Compliance**
 - Ensure secure handling of sensitive data, especially during next-of-kin verification and data transfer or deletion.
 - Invest in in-house security tooling and regular audits
 - Update privacy policies and terms of service to reflect UPAP processes.
- **Operational and Support Resources**
 - Customer Support
 - Process Management
- **Ongoing Maintenance and Updates**

6. Validation & Testing (PoC) for UPAP

What metrics will validate success?

For UPAP:

- How many SP implemented UPAP?
 - Without major issues?

For Service Providers:

- Death event handling accuracy
 - How many death request was actually false positives?
- Time to process requests
- User adoption — how many users actually sets up a emergency contact?
- Next-of-kin satisfaction
 - Relieve frustration in grieving period?

How will ethical risks be mitigated?

- Respect user wishes set pre-mortem
- Use of multi-factor to determine death
 - Avoid attacks targeted users that is still alive
- Ensure transparency in users wishes and ability to change those
- Take into consideration that emergency contact might be in a grieving period

Appendix C: Quantitative survey data

**Hvilken aldersgruppe tilhører du?**

140 of 140 answered

Pie chart

| | | |
|-------------------|-----|--------------|
| Under 30 år | 55% | 77 responses |
| 30 - 49 år | 22% | 31 responses |
| 50 - 69 år | 21% | 29 responses |
| 70 år eller ældre | 2% | 3 responses |

**Hvilken beskæftigelse har du?**

140 of 140 answered

Pie chart

| | | |
|----------------|-----|--------------|
| Fuldtidsansat | 46% | 64 responses |
| Studerende | 34% | 47 responses |
| Selvstændig | 9% | 12 responses |
| Andet | 6% | 9 responses |
| Arbejdssøgende | 6% | 8 responses |

**Hvor digitalt afhængig er din hverdag?**

140 of 140 answered

Pie chart

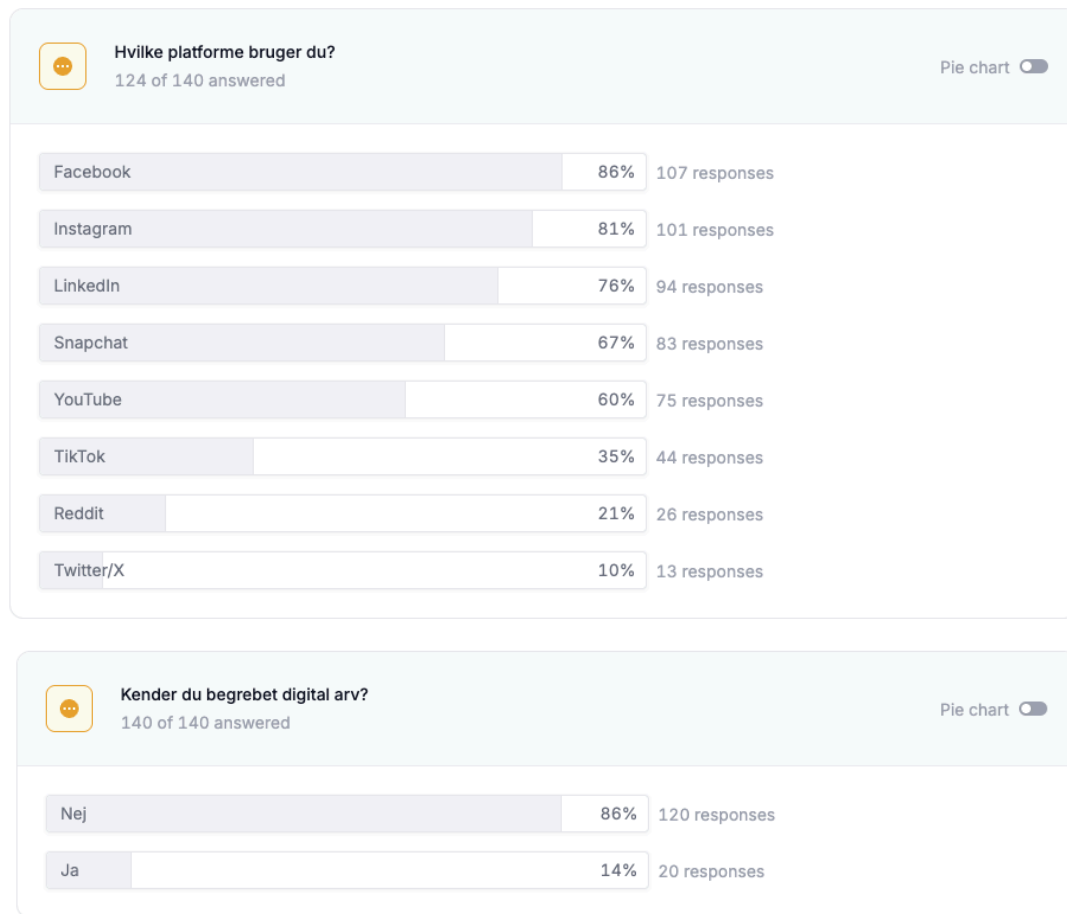
| | | |
|--|-----|--------------|
| Jeg bruger digitale løsninger til næsten alt. | 58% | 81 responses |
| Jeg bruger dem dagligt, men kan undvære nogle. | 37% | 52 responses |
| Jeg bruger dem kun, når det er nødvendigt. | 5% | 7 responses |

**Bruger du aktivt sociale medier?**

140 of 140 answered

Pie chart

| | | |
|-----|-----|---------------|
| Ja | 89% | 124 responses |
| Nej | 11% | 16 responses |





Hvordan vil du definere det med dine egne ord?

20 of 140 answered

| | |
|--|---|
| Hvad der findes af Data om os, efter vi er døde. | ⋮ |
| mit digital fodaftryk online efter jeg er væk | ⋮ |
| Jeg kan fx lade familie/venner overtage mine sociale medier via en fuldmagt man giver | ⋮ |
| udtryk, man bruger om de spor, som man efterlader på internettet efter ens død | ⋮ |
| Data som f.eks. online konti man efterlader efter sin død. | ⋮ |
| Families adgang til fx sociale medier efter ens død | ⋮ |
| De oplysninger, der findes om mig online. | ⋮ |
| Digital arv er alt det man efterlader sig digitalt efter døden. Det kan være profiler og opslag på SoMe, dokumenter på clouds, osv. | ⋮ |
| At man har formue i digitale verden | ⋮ |
| Adgang til digitale platforme efter død | ⋮ |
| Ryde min browser data | ⋮ |
| Det man efterlader, når man besøger en hjemmeside | ⋮ |
| Hvad der sker med dine digitale ting når du dør | ⋮ |
| Det digitale fodspor vi efterlader os, når vi dør. | ⋮ |
| Det digitale fodspor man efterlader tilbage efter sin død | ⋮ |
| En beslutning om hvad der skal ske med de digitale data efter døden! | ⋮ |
| At arve de digitale værdier men også at arve retten til de informationer der findes for den person som er død. Ikke noget jeg har hørt om i praksis, kun teoretisk | ⋮ |
| En mulighed for at håndtere data efter registrantens død. | ⋮ |
| Det digitale fodaftryk | ⋮ |
| Summen af digitale spor og indhold jeg har bidraget med og ikke ryddet op i | ⋮ |

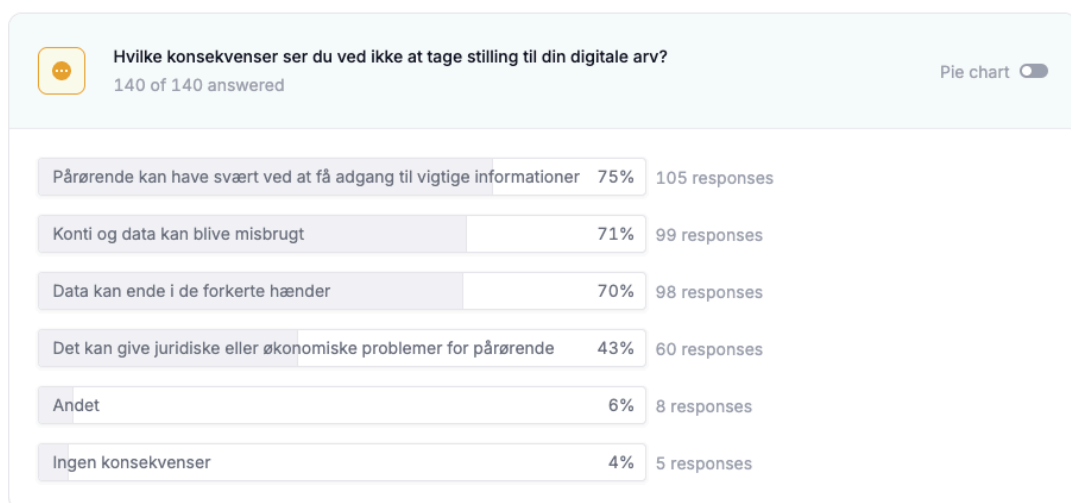
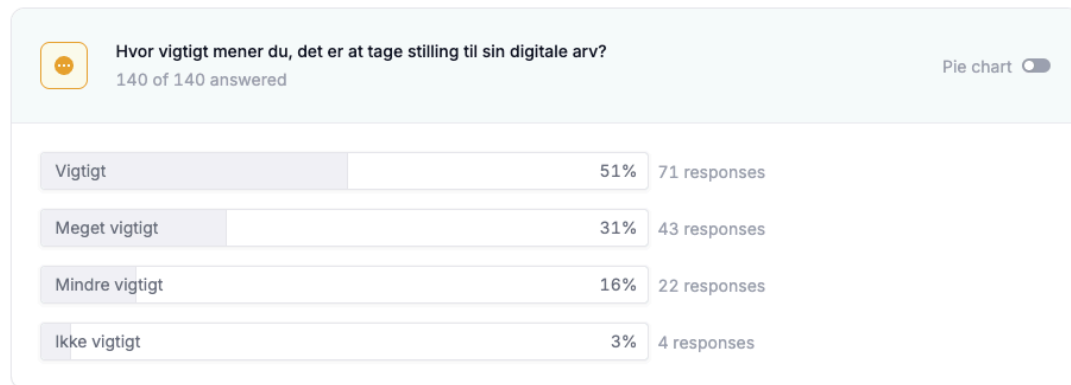



Har du tænkt over, hvad der sker med dine digitale data efter din død?

140 of 140 answered

Pie chart ☒

| | | |
|--|-----|--------------|
| Jeg har aldrig tænkt over det. | 51% | 71 responses |
| Jeg har tænkt over det, men ikke taget stilling. | 37% | 52 responses |
| Jeg er ikke bekymret for mine digitale data efter min død. | 10% | 14 responses |
| Jeg har overvejet det grundigt. | 2% | 3 responses |



 **Hvilke konsekvenser ser du ellers?**

8 of 140 answered

Private oplysninger ikke tiltænkt andre skal være utilgængeligt for alle

Jeg kan se at I har forholdt jer hovedsageligt til praktiske eller juridiske konsekvenser, men den følelsesmæssige påvirkning det har på de pårørende, når deres afdøde familiemedlemmer dukker op på sociale medier, er god at tage i betragtning. Det kan alligevel føles som et slag i maven, når Facebook pludselig minder én om at ønske dem tillykke med fødselsdage. Det har jeg selv oplevet gentagende gange.

Jeg vil gerne have at mine digitale fodspor forsvinder med mig og ikke have at de bliver hængende på forskellige platforme

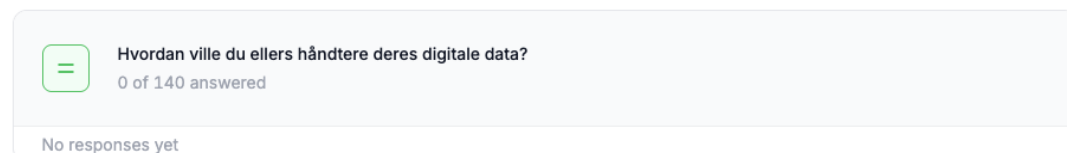
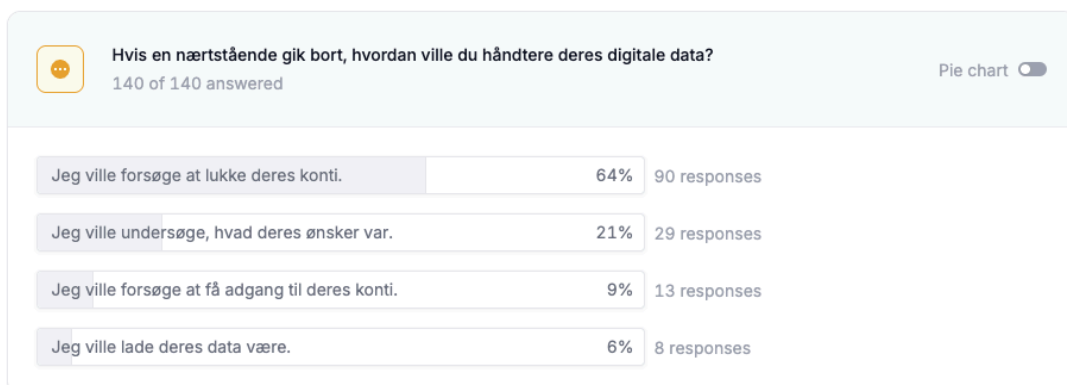
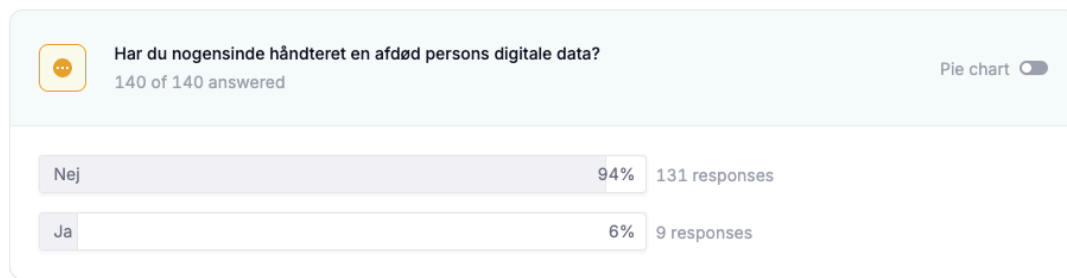
Pårørende kan blive mindet om dødsfaldet på en uheldig måde. Pårørende kunne føle sig forpligtet til at agere - hvis et "udsagn" om afdøde er forkert/provokerende

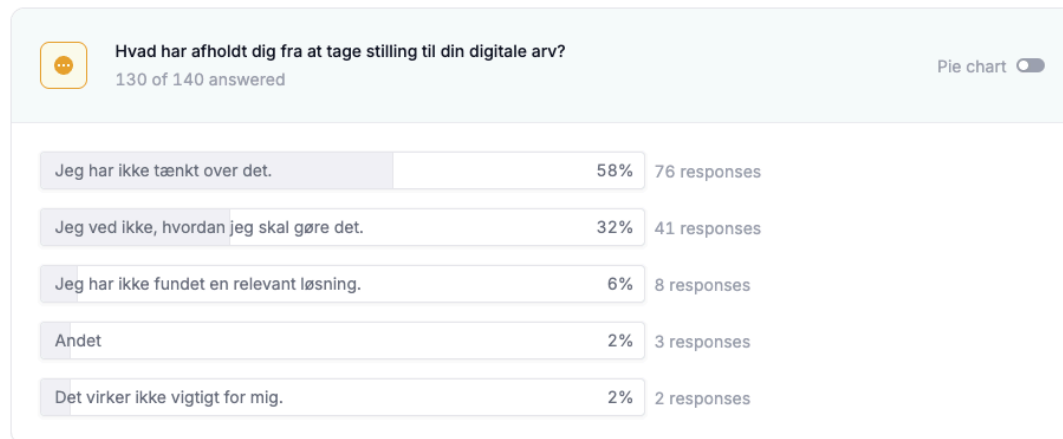
Hvis man har katte

Familiealbum kan gå tabt

For mig handler det mere om privatlivet omkring min "digitale data". Der er alt fra pinlige beskeder, mennesker man er i kontakt med i hemmelighed, forretnings data mm. Ting der kun er for en selv og aldrig har været tiltænkt deling med nogen som helst

I disse tider kan udseende og stemme misbruges med AI.



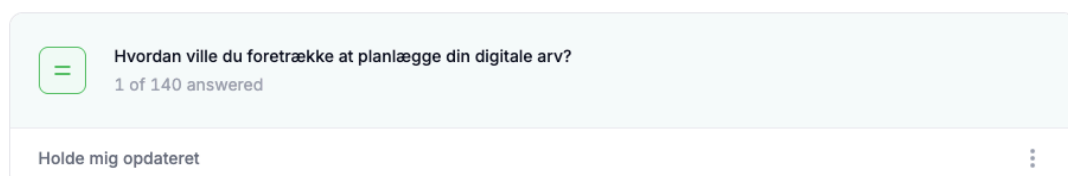
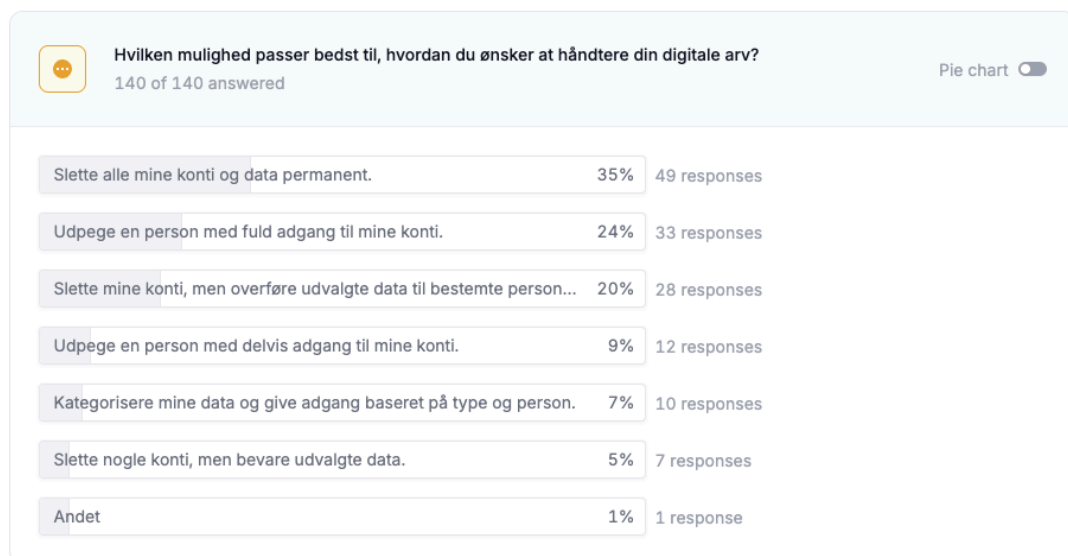
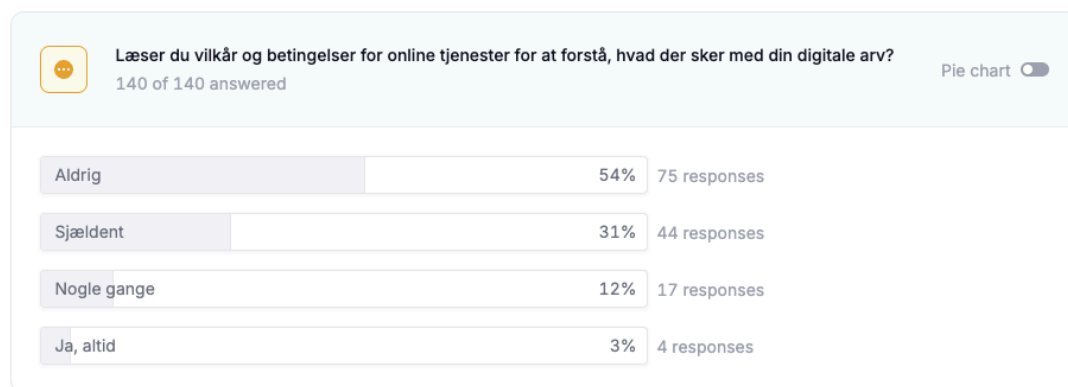
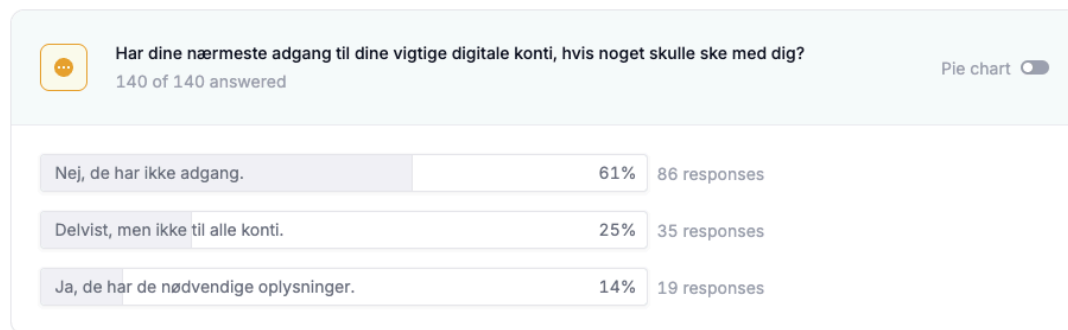


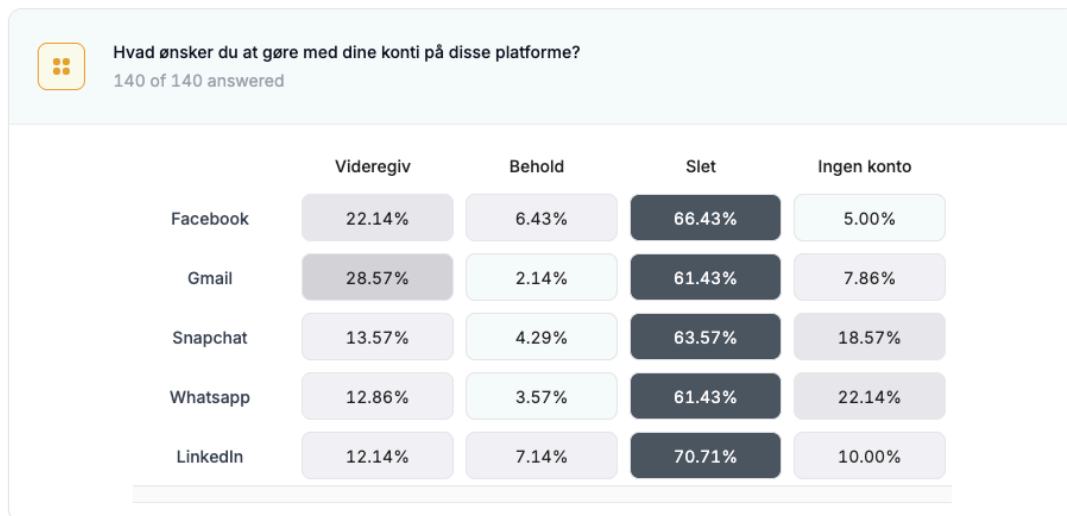
 **Hvad har afholdt dig fra at tage stilling til din digitale arv? (1)**
3 of 140 answered

| | |
|---|---|
| Magter ikke | ⋮ |
| Det ikke noget jeg har taget stilling til | ⋮ |
| Tvillinger på 2 år, ikke tid 😊 | ⋮ |

 **Hvilke foranstaltninger har du taget for at sikre din digitale arv?**
10 of 140 answered

| | |
|---|---|
| Skrevet koder ned. | ⋮ |
| Tilføjet min søster og mand som min arvekontakt gennem Apple, de vil få adgang til min iCloud data i tilfælde af død. | ⋮ |
| Jeg har givet e-mail og kode til en familiemedlem som jeg stoler på, og ved kommende er også min "legacy contact" på Facebook. | ⋮ |
| Skrevet hvem der har adgang til min profil via jeg dør (kan vist kun gøres på Facebook) ellers har jeg alle mine koder skrevet i min sidste vilje | ⋮ |
| Min datter har alle mine koder | ⋮ |
| Har adgangskode og private keys på et usb-stik i en kasse i mit hjem. Her ligger kode til min password vault samt en backup yubi key | ⋮ |
| Opsat familiemedlem som arving | ⋮ |
| Har udfyldt en erklæring på hvem der har adgang til mine Apple produkter efter død | ⋮ |
| Jeg har skrevet nogle ønsker ned som i første omgang er delt med min kæreste som kan anmode om adgang til min password vault | ⋮ |
| Gjort folk til pårørende f.eks. på min Meta for at sikre at andre har adgang. | ⋮ |







Har du yderligere kommentarer eller tanker om digital arv og håndtering af data efter døden?

14 of 140 answered

Kom til at tænke på at årsagen til ens død også har en betydning. Hvis man forsvinder eller myrdet, så det godt nogen har afgang til ens data

Adgang til aktiekonti burde også ske gennem digital arv

Jeg føler egentlig det er et rimelig vigtigt aspekt i det at have en online tilstedeværelse, at man ved hvad der sker, hvis man f.eks. skulle gå bort uden at være "forberedt" på det. Det er umiddelbart ikke noget, jeg har tænkt så meget over før, men jeg synes det er vigtigt, at der bliver kastet lys på det, og evt. skabt nogle muligheder for, at man som bruger af sociale medier kan have noget kontrol over, hvad der skal ske med sin digitale arv.

Nej

Jeg tænker, der er behov for oplysning om dette... havde ikke tænkt over det før nu!

God tanke

Det her er vigtigt, men også det med at snapchat ikke gad hjælpe med en hacked konto kan jeg genkende. Min Facebook blev hacked og det var kun med nød og næppe at jeg fik alt slettet. Jeg kender flere der lever med hacke somekontier og de kan ikke få hjælp.

Super vigtigt emne - tak for at tage det op.

Det er et svært emne, fordi det ikke er konkretiseret om vi faktisk ejer de data som vi stiller tilgængelige gennem forskellige tjenester. Der mangler regulering for at kunne understøtte digital arv i praksis, helt oppe fra EU niveau. Uden det vil tjeneste udbydere ikke røre en finger.

Vi undervurdere hvor meget følsom information vi har derude, det er noget der bør være regulativer omkring (evt krav om en person man vil videregive til når man opretter en profil), så det ikke kan blive misbrugt når døden indtræffer. Personligt vil jeg nu tage en samtale med mine forældre, søskende og min mand, så de ved hvad de skal gøre med min digitale arv og selv kan tage stilling til hvad de vil gøre med deres. Tusind tak for at belyse dette problem!

Nej, men jeg har nu taget stilling til det, så tak for indsigten. Rigtig fedt emne og tak for vigtig viden. Held og Lykke med jeres speciale, det kommer til at gå så godt! :)

Hva' sker der med min browser historik!?!?!?

Ja... wusssuuup!!

God undersøgelse, vigtigt tema som trænger orden og system.

