UNIVERSITY OF TWENTE.

Universität
Münster

Navigating Proportionality and Privacy: A Case Study of Technology Use in EU Border Management Systems

By
Hannah Broeknellis
Master Thesis
MSc European Studies & MA Comparative Public Governance
S2940213
Hannah.broeknellis@student.utwente.nl

Submitted in partial fulfilment of the requirements for the degree of Master of Science, program European Studies, University of Twente and Master of Arts, program Comparative Public Governance, Münster University

2025

Supervisors
First supervisor: Dr. Ola El- Taliawi
Second supervisor: Dr. Hendrik Meyer

Executive Summary

The increasing adoption of technological and Artificial Intelligence (AI) systems by public and governmental organizations raises concerns about the protection of fundamental and privacy rights of individuals. Especially, within the migration and border control sector, more technologies are being implemented to enhance the efficiency of migration processes. However, research shows that the fundamental rights of migrants are being harmed due to criminalization, discrimination, and increased surveillance (Amnesty International, 2024). As a results, the European Union (EU) has established regulations that govern data processing activities to safeguard the privacy rights of individuals. One of the most important principles governing these data processing activities is the principle of proportionality. However, concerns have increased regarding privacy rights due to the increasing data processing regulations, such as the principle of proportionality. As they try to increase privacy protection, it is often seen by public and governmental organizations as difficult to understand and how to implement in practice effectively. This study examines to what extent and how the principle of proportionality is included within the most relevant EU regulations and what gaps may exist that could harm privacy rights. Therefore, the research aims to provide policy recommendations and practical insights for public governmental organizations on how to implement and ensure proportionality standards when utilizing technological (AI) systems when processing personal data to protect privacy rights. The primary research question guiding this study is: *To what extent and how is proportionality embedded in the EU regulatory framework and how can it be enhanced to better align with public organizations' expectations and privacy protection when using (AI) technologies in border management?*

A qualitative research design was applied, combining a comprehensive literature review on legal requirements and a policy analysis on the EU regulatory framework combined with semi-structured interviews among relevant public governmental organizations, privacy experts, and humanitarian organizations. The results reveal that the principle of proportionality is formally embedded within the EU regulations, however, it lacks practical understanding and guidance. Moreover, requirements within the regulations are inconsistently applied, causing less deep ethical considerations when deploying technological (AI) systems. To address the main policy and practical gaps, a proportionality assessment and policy recommendations have been developed to safeguard privacy rights of migrants within the EU migration and border control sector in the future when using (AI) technologies.

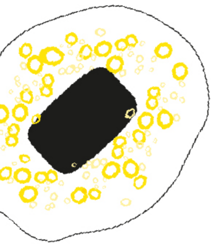
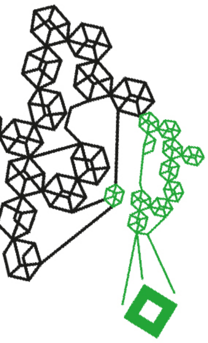
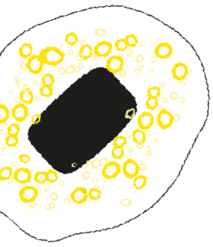
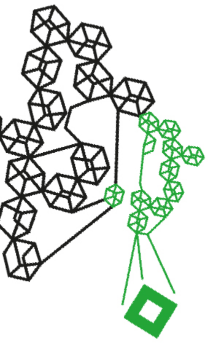


Table of Contents







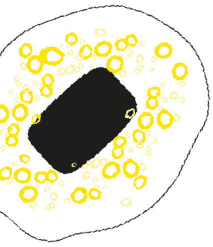
Glossary

AI	Artificial Intelligence
AI Act	Artificial Intelligence Act
CFR	The Charter of Fundamental Rights of the European Union
DPIA	The Data Protection Impact Assessment
EC	The European Commission
ECHR	The European Convention on Human Rights
EDPS	The European Data Protection Supervisor
EES	The Entry/ Exit System
EU	The European Union
FRIA	The Fundamental Rights Impact Assessment
GDPR	The General Data Protection Regulation
MS	Member States
NGO	Non-Governmental Organization
SIS	The Schengen Information System
TEU	The Treaty on European Union
VIS	The Visa Information System

1. Introduction

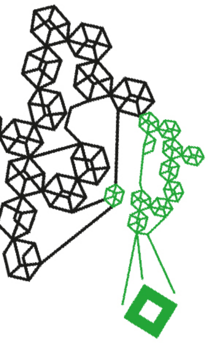
Technologies are not new in modern society and are used for everyday practices. Among these technological innovations, so-called Artificial Intelligence (AI) systems are being developed. Numerous organizations increasingly use both technological and new AI systems to enhance their operations and processes. One important sector that has been developing AI technologies significantly over the last few years is the migration sector, which tries to manage migration flows at borders. The technological (AI) systems could potentially enhance the speed of border controls and application procedures while respecting the human rights of the people (Forti, 2021). Therefore, more and more European Union (EU) states are incorporating these technological (AI) tools into the management of their migration flows. Examples of these technological tools include facial recognition, fingerprints, biometric scanners, infrared cameras, and other automated data collection mechanisms (Forti, 2021). However, the integration of these technologies in the context of border controls is raising questions and concerns that are necessary to address. Many human rights organizations, such as Amnesty International (2024), have studied the violation of human rights and privacy at borders related to the use of technologies by states. Their report highlights that while these technologies intend to enhance the efficiency of border controls, they can also lead to criminalization, discrimination, and increased surveillance of travelers and migrants leading to increased vulnerability and infringement on human rights and privacy.

The infringement of privacy is primarily abused by the extensive processing of personal data within these systems, since migrants are asked to hand in a significant amount of this personal data. Personal data can include date of birth, full family names, country of origin, gender, criminal records, and biometric data. Consequently, personal data is being processed to train algorithms, which drive AI-systems to assess the risk level of a passing individual, resulting in granting or denying access to the EU. The personal data obtained is then registered and screened within various databases across the Member States (MS). This results in an increasing number of privacy and data protection violations and raises questions about proportionality (Statewatch, 2023). In addition to the use of technology in border management systems, many other (public) organizations are incorporating (AI) technologies into their systems to improve efficiency and streamline operations. Also here, concerns arise about the balance between the substantive proportionate processing of personal data while maintaining privacy standards (European Parliament, 2020). To ensure that proportionality is guaranteed, the Treaty on European Union

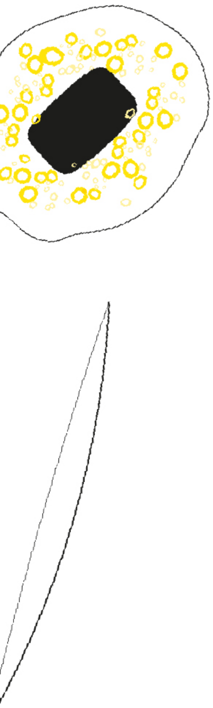


established a standard on the principle. This principle requires that personal data processed by technological systems must be relevant, adequate, and strictly limited to what is necessary for the intended purpose (European Data Protection Supervisor, 2024). Although this appears to be a logical principle, there is, in practice, a lack of clear guidance on how organizations and MS should assess the proportionality of personal data processed by technological systems at the borders (McGregor & Molnar, 2023). As a result, it has been demonstrated that the effects of technologies on human beings are not adequately examined and assessed, emphasizing the critical need for a balanced approach that prioritizes proportionality in the development and use of technological (AI) systems at borders (Warthon, 2024). However, a thorough proportionality assessment within technological systems has yet to be adequately investigated or developed by the relevant authorities of involved countries within the EU, even when concerns about privacy rights breaches are currently highly politicized (Alarcón et al., 2024).

Multiple European risk assessments, including the so-called Fundamental Rights Impact Assessment (FRIA) and the Data Protection Impact Assessment (DPIA), have been established to assess the high risks of technological border systems that could affect privacy and other fundamental rights (Delinavelli, 2023). Although these assessments are looking promising, they are falling short in addressing proportionality risks. For example, the FRIA aims to evaluate the impact of AI-systems on fundamental rights, yet it falls short of guidelines that measure and ensure proportionality in practice. In addition, this risk assessment is only applicable to *high-risk* AI-systems and only assesses this system *before* the system is installed (Ajoodha & Browne, 2025). This is concerning, since the amount and type of data processing changes over time, meaning that these systems could potentially harm privacy rights in the future (Haefner et al., 2023). In addition, the high-risk categorization as described by the AI Act excludes the AI-systems used at borders, therefore, these systems do not have to comply with the Act for the upcoming years (Bouvier, 2024). As a result, while these assessments show important steps toward safeguarding privacy rights, there remain significant concerns about their ability to operationalize proportionality principles effectively. These concerns highlight the urgent need for enhanced guidelines that can provide clearer guidance on how to assess and implement proportionality standards when using (AI) technologies, particularly in sensitive and highly politicized areas such as border management (Alarcón et al., 2024).

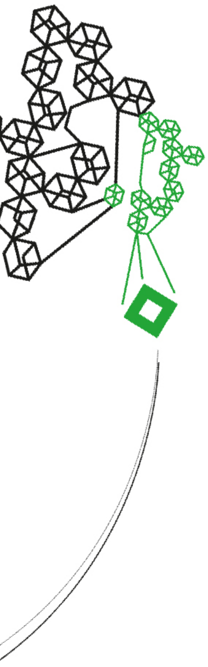


1.1 Relevance



Scientific relevance

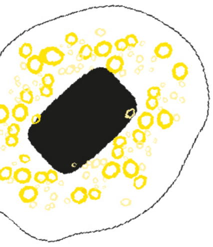
This study intends to contribute to a more comprehensive understanding of the deployment of (AI) technologies, highlighting the regulatory improvements and guidelines required to ensure proportionality and thus privacy rights within such systems. The study will explore the regulatory framework governing (AI) technologies at EU borders, specifically examining the extent to which the proportionality principle is implemented in practice and to what extent it safeguards the privacy rights of migrants. Although the principle of proportionality is legally embedded within the EU regulatory framework, there remains a lack of clarity and academic consensus on how to implement the principle in practice (Kloza & Drechsler, 2024). The EU established risk assessments falls short on this operationalization. Therefore, the research will try to identify the essential and needed components governing proportionality within the EU regulatory framework and such an assessment, help guide organizations on how to effectively protect the personal data processing of migrants when using technological (AI) systems. Consequently, the study is addressing a critical research gap in the field of digital governance and privacy law in a highly sensitive public area.



Societal relevance

As seen in the literature, the integration of technologies within border management has significant implications for human rights, in particular for the privacy rights of migrants (Amnesty International, 2024; Statewatch, 2023). The expectations and practical implementation of proportionality by relevant governmental organizations will be examined to identify the gaps and necessary improvements. While not all organizations may explicitly advocate for migrant rights, there is a growing recognition of the importance of ethical considerations while implementing (AI) technologies (Haefner et al., 2023). Therefore, understanding the expectations and experiences of these organizations regarding proportionality and, thus, safeguarding privacy rights when implementing (AI) technologies is crucial for this research.

1.2 Research aim and questions



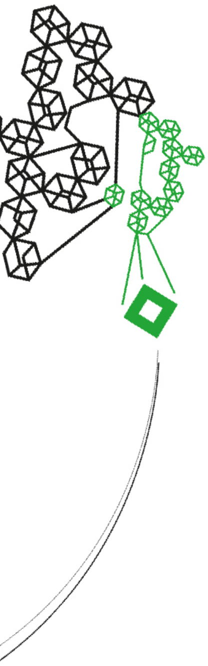
Using the case study of (AI) technology used in EU border management, the research seeks to offer practical insights for organizations on how to implement and ensure proportionality standards when using technological systems and processing personal data to safeguard privacy rights. To achieve this, the following main research question and research sub-questions have been established.

Main research question

To what extent and how is proportionality embedded in the EU regulatory framework and how can it be enhanced to better align with public organizations' expectations and privacy protection when using (AI) technologies in border management?

Sub-questions

1. How is the proportionality principle embedded within the EU regulatory framework?
2. What are the gaps regarding the proportionality inclusion within the EU regulatory framework compared to the practical implementation?
3. Do the relevant public and humanitarian organizations' expectations align with the EU regulatory framework?
4. What guidelines are necessary to enhance proportionality implementation when using (AI) technologies to protect privacy rights effectively?



The first sub-question is essential for a comprehensive understanding of the current EU regulatory framework covering (AI) technologies at the EU borders. This question creates an understanding of the current legal base covering the proportionality principle and, therefore, privacy rights. Inclusion refers to the scope of governance and regulation that the EU aims to establish within its regulatory framework concerning proportionality standards. This legal base is essential for answering the second sub-question, which will investigate the gaps. The gaps refer to the difference between the inclusion of proportionality in the EU regulations and the degree of practical implementation of these proportionality standards in the EU border management context. Identifying these gaps is critical for understanding where improvements are needed. In addition, the third question will try to identify the expectations towards the EU regulatory framework governing the data processing of relevant public and humanitarian organizations in the migration sector. The research aims to examine to what extent these organizations understand the proportionality principle, what they expect to be included within the regulations, how they try to comply with the EU regulations, and how they ensure privacy rights for migrants. Moreover, this research seeks to understand the views of privacy experts and humanitarian organizations to establish comprehensive recommendations for the implementation of proportionality.

As a result, the second and third sub-questions will identify gaps and needs in the inclusion of proportionality in the EU regulatory framework, which will serve as a framework for the final question. The final question will attempt to develop a set of guidelines to address the gaps and expectations highlighted. As a result, the guidelines will assist organizations in better understanding how to comply with proportionality standards and adopt them in the future when incorporating (AI) technologies into their processes. These guidelines will help other companies to safeguard and successfully execute proportionality following EU legislation when considering and implementing (AI) technologies.

1.3 Structure

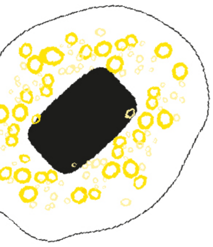
The thesis is structured into different chapters, as follows. The first chapter consists of the *Literature Review*, which describes earlier investigations on the topic and highlights the relevance of this research. The second chapter presents the *Theoretical Framework*, covering the main concepts and frameworks, along with the conceptual framework and an explanation of the key concepts. This is followed by a description of the *EU border management Case Study* chapter. Next, the *Methodology* chapter outlines the research design, operationalization of the key concepts, and explains how validity and reliability will be ensured throughout the research. The fifth chapter shows the *Results* after data collection has been completed, aiming to answer the research questions. Finally, the last chapter includes the *Conclusions and Discussion*, as well as any implications remaining from the research.

2. Literature review

Finding previously developed research on (AI) technology integration in border management can be challenging due to the relatively recent nature of the topic. However, increasing research is being conducted regarding human rights infringements related to AI systems. Therefore, this literature review evaluates the existing studies that have examined the impact of (AI) technologies on privacy and proportionality standards and identifies gaps relevant to this research.

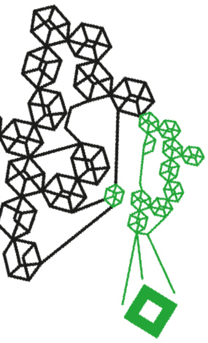
Both the EU and the US have intensified their efforts in border management to mitigate security risks and enhance efficiency. This is a process of "smartening" their border management, which includes the integration of technologies and the development of AI systems. Technologies come in multiple forms and have been in place for over a decade. The most recent technological developments also include AI features, introducing radars, drones, biometric systems, and satellite data systems. These systems are, for example, placed at the seacoast to monitor crossing migrants (Frontex, n.d.). The primary objective of these technologies is to improve the effectiveness of border control. This includes increased technology testing, relying on profiling conducted through algorithms, and the utilization of surveillance tools on travelers and migrants. Consequently, the EU has assigned significant mandates to relevant EU border agencies to test and implement these technologies (Gandhi, 2024). A study by Nalbandian (2022) investigated the case in the United States (US), which is implementing technologies at its borders to enhance its border security, but mainly to prevent illegal migrant movements. In 2018, the US developed a new biometric database called the Automated Biometric Identification System, asking migrants for facial images, fingerprints, iris scans, and information about their sex, criminal records, and other personal history. Additionally, the US is also gathering data from public resources to expand its knowledge and data. The public data, together with other gathered biometric data, is used by machine-based learning technologies to identify patterns of criminal activities. The US institutions are receiving more funds nowadays to expand their mandates and data collection methods for border management technologies.

Although AI promotes itself as a tool for supporting the implementation and delivery of immigration rules and initiatives, its use will have negative consequences on migrants, particularly refugees and asylum seekers. Nations that aim to balance security and efficiency, like the EU, could give in to the interest of AI, which can have unintended negative consequences for migrants. States with anti-immigration policies, like the United States, may not prioritize the rights of irregular migrants, leading to severe consequences for those most vulnerable to these (AI) technologies (Nalbandian, 2022).



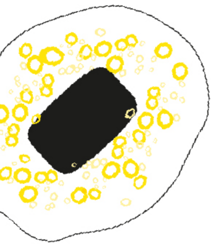
Human rights violations

According to a study by Amnesty International (2024), these consequences lead to human rights breaches, as can be seen in the following example. The EU helps Libyan authorities by providing resources, training, and coordination, allowing Libyan coastguards to intercept boats and return migrants and refugees to Libya. This is accomplished through the use of aerial surveillance, including drones operated by Italy and Frontex, to spot boats and alert Libyan authorities, leading to their interception. When these migrants return to their original country, these migrants face detention, torture, sexual violence, and other abuses. Beyond physical breaches, these technologies raise concerns about discrimination, algorithmic bias, privacy violations, and broader human rights infringements, particularly regarding the massive collection and processing of (sensitive) personal data. When algorithms work with biased data, they produce biased outputs. This is particularly concerning with innovative migration technology. For example, an AI-powered lie detector is being tested at airports in Hungary and Greece. The algorithm examines passengers' facial expressions and, if it senses suspicion, the system assigns the passengers for further screening by a human officer. However, AI may have difficulty accounting for cultural differences or memory impairments among asylum seekers. Furthermore, facial recognition frequently misidentifies women and people of darker skin tones (Molnar, 2024).



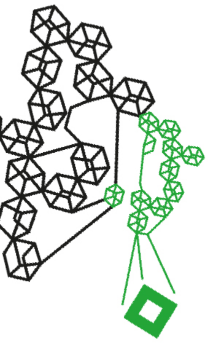
Another recent study by Peerboom (2022) highlights the fact that the EU has a strong tendency to prioritize border security above the privacy rights of migrants. Critical mistakes are made in safeguarding and informing migrants about their privacy rights. These rights include the right to data protection, to access the data, to make decisions themselves, and to have insight into how their data is being processed. In addition, there is a lack of accountability, a lack of algorithm transparency, and a lot of cybersecurity vulnerabilities appear. The literature emphasizes the urgent need for measures to protect the privacy rights of migrants from the EU and its MS. Despite these concerns, the EU continues prioritizing the protection of its borders over migrants' privacy (Peerboom, 2022). Therefore, Molnar (2023) calls for further investigation on how the EU should create a "*commitment to a human-rights-based approach to the development and deployment of border technologies*".

Proportionality standards



As a response to the existing research about human and privacy rights infringements, the EU has established the EU Artificial Intelligence Act (the EU AI Act) to protect these. However, research has shown that the Act is not sufficient to protect the privacy rights of migrants because of the lack of an understandable framework to assess proportionality. To understand the gaps in the literature, the principle of proportionality will be explained shortly.

Proportionality is a principle that goes way back before the existence of technological and AI applications. It has always been a general standard within the law and governing of the EU. In the broader and more general EU context, it refers to the restriction of authorities to exercise their powers. This results in forcing authorities to balance their use of measures with the proposed aim. In addition, they need to clarify that the measures they would like to implement must be necessary for the aim, and they should not impose any individual rights (European Union, 2024). In the context of privacy rights, proportionality is necessary for safeguarding the processing of personal data, since it serves as a limitation for data collection (European Data Protection Supervisor, 2024). When any (AI) technology is, in some way, restricting the rights of privacy, proportionality ensures that these restrictions on the rights must be fair, and the measures taken when using (AI) technologies must be suitable for achieving the intended goal. Thus, when evaluating the processing of personal and biometric data, proportionality commands that only the personal data necessary and relevant for the intended purpose should be collected and processed (Karliuk, 2022; European Data Protection Supervisor, 2024). The author Karliuk (2022) mentions the concerns regarding the practical implementation of the proportionality principle. For instance, how organizations can ensure that the use of technological (AI) systems remains within the necessary limits and ensure that no excessive constraints are placed on marginalized individuals, such as migrants. The specific way proportionality functions and how it should be implemented correctly is still a topic of intense discussion within the academic world and has not been researched well yet (Kloza & Drechsler, 2024).



The existing literature emphasizes the ethical and legal problems created by technology (AI) usage in border management, particularly in terms of human rights, privacy, and proportionality. However, there is a lack of research looking into how proportionality might be properly implemented within border management. This study intends to contribute to this discussion by investigating how to create a more human-centered legislative framework in the EU. Ensuring that technology use is consistent with fundamental rights and privacy laws, and in particular, complying with and the right implementation of the proportionality standard.

3. Theoretical framework

3.1 Artificial intelligence

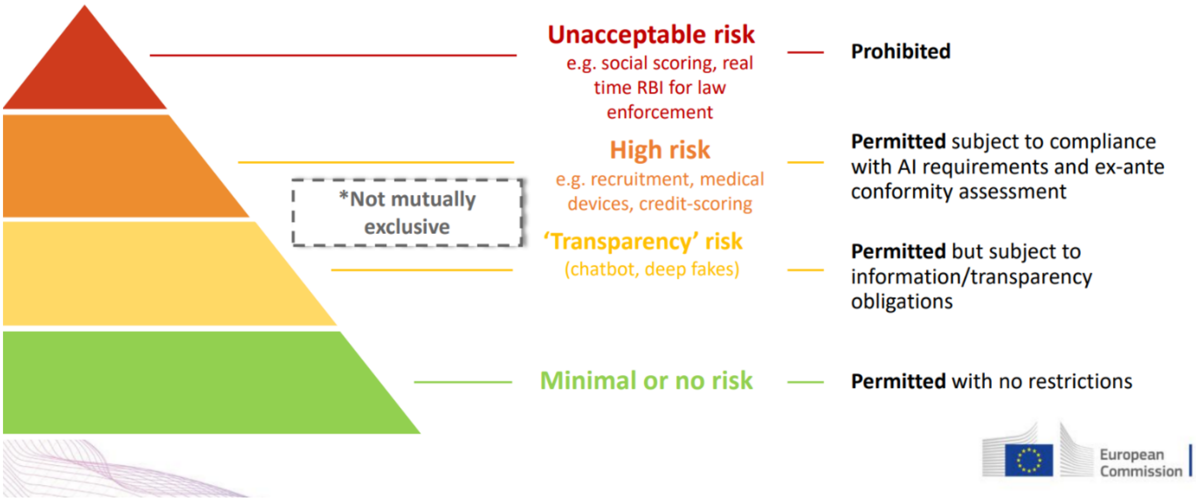
Definition

There is no global consensus over a definition for AI because it encompasses multiple technologies and systems with diverse methods and applications. However, the new EU Artificial Intelligence Act (2025) has tried to create the following broad definition for AI in Article 3: *"AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".* To clarify this further, the EU AI Act has established key characteristics that divide the definition of AI, including machine-based learning, varying levels of autonomy, adaptiveness, use of AI techniques, generating output, and influence on physical and virtual environments. In the context of border management systems, AI refers to technologies and algorithms that assess individuals passing the EU borders and therefore enhance the speed of border controls. The assessment is focused on the extent the which passing individuals pose a risk to public security, if these individuals are part of irregular migration, and therefore trying to predict individuals' traveling behaviors (Vavoula, 2021). This analysis is done through multiple algorithms that collect, examine, and evaluate a significant amount of data about travelers, such as information on visa applications, travel patterns, and biometric data. Consequently, the algorithms collect and process personal data, which is able to read through millions of data sets of macro-level travel information (Belderbos, 2025).

Classification of AI systems

The EU AI Act (2025) has established a framework to distinguish between four types of AI systems to identify the associated risks and impacts these systems create when collecting and processing personal data. The higher the classification of the type, the stronger the regulations and requirements will be. The Act distinguishes between "Unacceptable Risk", "High Risk", "Limited Risk", and "Minimal Risk" as can be seen in Figure 1 below. This figure was established by the European Commission in 2022 and is comprehensive in showing the risk categorization. However, currently, the "Transparency Risks" as shown in the figure of the European Commission are now named as "Limited Risks" within the AI Act.

Figure 1: The EU risk categorization for AI systems


Unacceptable risk
e.g. social scoring, real time RBI for law enforcement
Prohibited
High risk
e.g. recruitment, medical devices, credit-scoring
Permitted subject to compliance with AI requirements and ex-ante conformity assessment
*Not mutually exclusive
'Transparency' risk
(chatbot, deep fakes)
Permitted but subject to information/transparency obligations
Minimal or no risk
Permitted with no restrictions
European Commission

(European Commission, 2022)

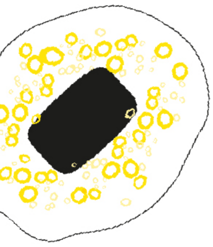
To understand the different AI technologies and the extent they require compliance with the AI Act, a short description of each category will be given. This will also help understand how proportionality plays a role in the AI Act, ensuring that the level of oversight and compliance requirements is appropriate to the potential risks associated with each type of AI system. By categorizing AI technologies based on their risk levels, developers and providers can better navigate the regulatory landscape and implement necessary measures to mitigate the risks (EU Artificial Intelligence Act, 2025).

Unacceptable risk – Banned AI systems

Article 5 of the AI Act describes which AI systems are a significant threat to society and their fundamental rights and therefore are banned from being used. The systems include for example social scoring systems and manipulative AI systems, such as real-time biometric identification systems in public spheres (EU Artificial Intelligence Act, 2025).

High risk – Compliance

Most of the AI- systems used will fall around the high-risk systems, therefore, the AI Act revolves around these systems as described in Article 6 of the Act. Examples of these systems can include biometrics, infrastructure, education, law enforcement, migration and border control management. These systems are classified as those that are likely to adversely affect the safety or fundamental rights of EU citizens. It is essential to evaluate the anticipated risks before these systems are introduced to the market and continuously throughout their development. They require strict compliance with the AI Act and providers of the system should be responsible for ensuring this compliance (EU Artificial Intelligence Act, 2025).



Limited risks– Transparency

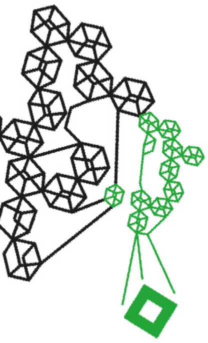
AI systems that pose a limited risk (as described in Article 52 of the AI Act), such as systems that interact with humans (e.g. chatbots), emotion recognition systems, biometric systems, and categorization and AI systems that generate or manipulate images, audio, or video material, will have to comply with a limited set of transparency obligations.

Minimal risks – Unregulated

All other AI systems that pose only a low or minimal risk (as described in Article 69 of the AI Act) may be developed and used without complying with additional legal obligations under the AI Act. Nevertheless, the European Commission encourages providers of AI systems to voluntarily meet the mandatory requirements for high-risk AI systems (EU Artificial Intelligence Act, 2025).

3.2 Proportionality principle

To ensure that personal data is handled according to EU standards and privacy rights are safeguarded, the so-called proportionality principle has been established by European law, under the Treaty of European Union (TEU) in Article 5. They defined the principle of proportionality as (The Treaty of European Union, 2012).



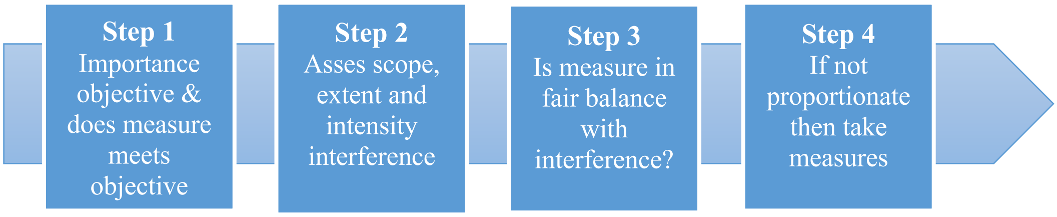
> *"The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties."*

The principle of proportionality is enshrined in multiple legal systems and different (national) regulations across the world. It is used to guide decision makers in order to create more justifiable and morally acceptable decisions. These considerations can therefore be applied to technological (AI) systems, and consequently, the principle of proportionality could be very important and useful when looking at ethical considerations (Karliuk, 2022).

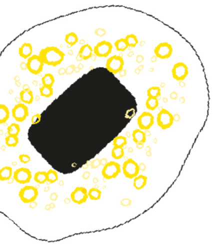
As can be seen, proportionality remains a subjective concept, meaning the concept can be interpreted in many ways, therefore making it difficult to define and measure it (Pass, 2024). This problem is also one of the main reasons why this research is conducted. To investigate what the standards are, how relevant public organizations understand the concept and under which circumstances, interviews will be held to get an understanding. Due to the different actors involved in the research (governments, public organizations, migrants, and non-governmental organizations (NGOs)), different interests apply. Governments' interests lie in the face of prioritizing innovation, security, economic growth, and controlling their borders over the regulation of privacy protection when using AI technologies. On the other hand, migrants' and NGO's interests lie in prioritizing their (migrants) safety and maintaining privacy rights (Zaidan & Ibrahim, 2024). Public organizations are between trying to safeguard privacy rights and trying to be compliant with EU regulations, avoiding any sanctions while optimizing their processes with AI. Therefore, it is necessary to find a balanced way in which the multiple interests are considered when regulating proportionality.

The European Data Protection Supervisor (EDPS) (2019) has created a so-called "proportionality test" which organizations can consult when considering and implementing new (AI) technologies. The steps underlying this test are shown below in Figure 2. In short, these steps include: 1) Firstly, assessing the importance or the legitimacy of the goal, and to what extent the taken measures are meeting the goal. 2) Secondly, assessing the intensity and scale of the measure, understanding how the measure could affect privacy rights and should not put an excessive burden on the individual. 3) The third step includes the proportionality principle, meaning finding a balance between the extent of the measure and the constraints this will have on privacy rights.

Figure 2: Proportionality test

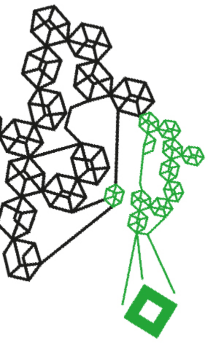

Step 1
Importance objective & does measure meets objective
Step 2
Asses scope, extent and intensity interference
Step 3
Is measure in fair balance with interference?
Step 4
If not proportionate then take measures

Also, within this framework, it is not clear where this balance lies and which/when a right is violated. The EDPS (2019) instructs organizations to compare the constraints and benefits for themselves, which is very inconsistent and unclear. This research will therefore try to find an answer to this question of how organizations can interpret this comparison and be compliant with the regulations of proportionality. 4) The last step refers to taking suitable actions/changes to make sure the taken measures are appropriate and safeguard the rights of the individuals.



3.3 Defining rights

In this research, numerous concepts regarding fundamental rights, human rights and privacy rights are being given. Therefore, it is essential to clarify the distinction between these rights and specify which rights this research will focus on. Fundamental rights are rights that are determined and written down within the constitutions of each country but also should align with the overarching fundamental rights stated in the Charter of Fundamental Rights of the EU (CFR) & the European Convention on Human Rights (ECHR) (European Union Agency for Fundamental Rights, 2020). These fundamental rights include the right to freedom, democracy, equality, and the rule of law, which are legally enforceable. Therefore, this can result in citizens facing prosecution by the court when violating one of these rights (European Parliament, n.d.). In addition to the fundamental rights, there is a set of so-called human rights that are incorporated into national laws. However, human rights cover more universal rights that apply to any individual, regardless of country of origin, religion, or age. These rights overlap with fundamental rights but are less specific and more focused on ethical considerations, such as privacy rights (Rehman, 2022). Consequently, privacy is a right that will both fall under fundamental and human rights since it is integrated into the EU constitutions and national laws. The right to privacy entails control over your own identity, choices and maintaining autonomy (Kumar, 2023). Within this research, the focus will lie on these privacy rights. The exact dimensions of privacy will be further explained within the Conceptualization chapter.

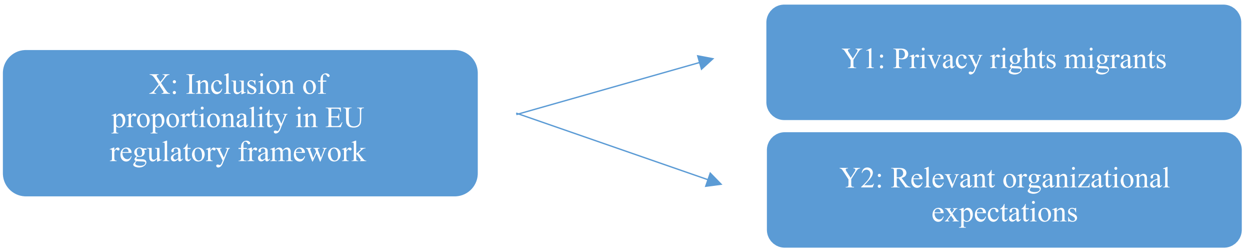


3.4 Conceptual framework

This section covers the key concepts related to the main research and sub-questions. It will explain the conceptualization and dimensions of each concept. The key concepts in this research include 1) *the inclusion of the proportionality principle within the regulatory framework of the EU* governing the use of (AI) technologies in border management, 2) *the privacy rights of migrants*, and 3*) the relevant organizational expectations* surrounding proportionality implementation when applying AI systems. The inclusion of proportionality within the EU regulatory framework can be divided into two parts. The first part relates to the proportionality principle and the second to the EU regulatory framework concept. Proportionality, in short, involves ensuring that the data collected by any technological (AI) system is relevant, adequate, and only used for the intended purpose (European Data Protection Supervisor, 2024). The second part relates to the regulatory framework of the EU, which is defined as all regulations governing technology usage within border management that create rules on regulating the processing of personal data and privacy rights. The third variable, relevant organizational expectations, refers to how both public and humanitarian organizations perceive and act upon the inclusion of the proportionality principle within the EU regulatory framework. This also encompasses how and to what extent these organizations understand the proportionality principle, how they implement the principle in practice, and identify any gaps that may exist. Moreover, it is examined to understand how humanitarian organizations perceive the regulatory framework and what effects it might have on safeguarding the privacy rights of migrants.

To examine the relationship between the three variables, a conceptual framework has been established. A cause-and-effect relationship will visualize the three concepts and show the effect the independent variable has on the two dependent variables within the research (George, 2024). The integration of proportionality in the EU regulatory framework could potentially affect the privacy rights of migrants but also affect the public expectations towards AI systems used at border controls. Therefore, the independent variable is the inclusion of the proportionality principle integrated into the EU regulatory framework and the dependent variables are the privacy rights of migrants and the public expectations regarding proportionality standards. A negative impact is expected between *the inclusion of the proportionality principle within the regulatory framework of the EU* and *the privacy of migrants* since till today it has become clear that the EU is still prioritizing the security of borders over the privacy rights of migrants and it is expected that the privacy rights cannot be ensured through the already established proportionality assessments (Peerboom, 2022; (Kloza & Drechsler, 2024). In addition, a negative impact is expected between *the inclusion of the proportionality principle within the regulatory framework of the EU* and the *relevant organizational expectations*, since the proportionality principle is covered within the EU framework, however, the concept can be interpreted in many ways and doesn’t operationalize a proportionality assessment for organizations. This causes organizations to struggle with how to effectively understand and implement proportionality, therefore, leaving certain gaps in how to balance the processing of personal data while safeguarding privacy principles.

Figure 3: Cause and effect relationship



X: Inclusion of proportionality in EU regulatory framework

Y1: Privacy rights migrants

Y2: Relevant organizational expectations

Hypotheses

In addition to the overall cause-and-effect relationship, hypotheses per sub-question have been established to measure the relationship between the variables within the questions. The hypotheses will be used to answer the questions in the results chapter. Question 4 will not have a hypothesis, as it does not aim to test an assumption but instead seeks to establish practical guidelines based on the findings derived from the other sub-questions. The hypotheses per sub-question are as follows:

RQ 1- *H1: The principle of proportionality is formally included within the EU regulatory framework but is missing regulatory guidance for practical implementation.*

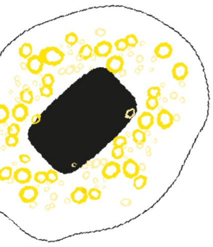
RQ 2 - *H2: There are significant gaps between the proportionality inclusion within the EU regulatory framework and the practical implementation.*

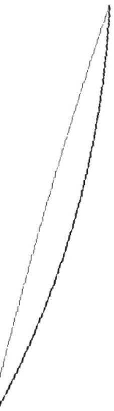
RQ 3 - *H3: The expectations of relevant public and humanitarian organizations do not align with what is stated in the EU regulatory framework, therefore, these organizations do not know how to effectively safeguard privacy rights.*

3.5 Conceptualization

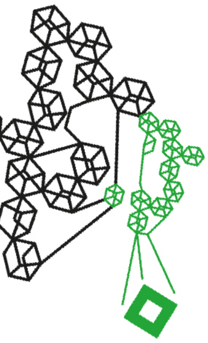
To create an understanding of the independent variable, **1) the inclusion of the proportionality principle within the EU regulatory framework**, the concept will be divided into two parts. The first part is the *EU regulatory framework,* which refers to a set of rules, laws, and guidelines established by the EU government to oversee and control various aspects of an activity or sector within the MS. These frameworks are designed to ensure compliance with standards, protect rights, and outline the responsibilities of different MS (*What Is The EU Regulatory Framework? 2*024). The EU's regulatory framework regarding governing the use of AI tools on border management systems, focusing on safeguarding privacy rights, consists of two main regulations that will be assessed during this research.

The European Commission started establishing soft laws, including guidelines on the use of AI systems, but shifted towards a legislative strategy, incorporating harmonized rules on AI technologies (Madiega, 2024). One of these important regulations is the so-called General Data Protection Regulation (GDPR), which has been binding for MS since the year 2018 (European Data Protection Supervisor, 2018). The GDPR is a comprehensive regulatory framework defining the fundamental and human rights of migrants, obligations for processing data, and

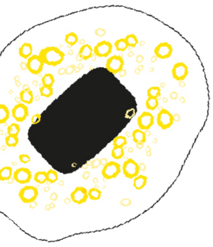




methods ensuring compliance (European Council, 2024). Its main goal is to focus on improving the coordination of information transfers across borders and improving effectiveness regarding the protection of personal data and privacy rights within EU countries (Shabani & Borry, 2017). The second and most recent important act is the EU AI Act, as mentioned before. The AI Act is a worldwide regulatory framework describing a set of rules regarding the development and operation of AI technologies in a responsible manner by organizations, public institutions, and governments. It entails requirements to make sure the AI is safe, transparent, and non-discriminatory (European Parliament, 2023) since some of these risks have not been sufficiently covered by the GDPR. It will, for example, safeguard that risks are considered by AI developers and create classifications for each AI system based on certain risk groups, ranging from low to high risk (Autoriteit Persoonsgegevens, 2025). These regulations form a comprehensive regulatory framework, which encompasses the most recent important regulations and acts related to protecting privacy rights. The attributes or dimensions of a regulatory framework include the regulatory purpose, the scope of the regulation, rules, and implementation mechanisms. The regulatory purpose can be understood as the primary objectives and goals the regulatory framework tries to achieve regarding using AI at borders safely within the EU (Hadley, 2022). The scope of the EU regulatory framework can be understood as the extent and boundaries of the regulation, including the activities and geographic areas it will apply to (*OECD*, 2015). In this case, the scope will focus on the EU and its borders. The rules refer to the specific guidelines, criteria, and standards that must be followed by the EU countries (Data Guard, 2024). Lastly, the implementation mechanisms can be understood as the processes established by governing bodies of the EU, including institutions and authorities, for overseeing compliance and enforcing regulations through monitoring and enforcement procedures (Better Care Network, 2023). These dimensions will define and differentiate the two regulatory frameworks being studied.

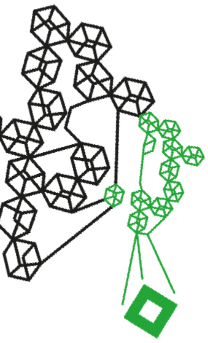


The second part is the *proportionality principle*. The author Karliuk (2022) defined proportionality within the general and AI context, which will be used in this research. The general meaning of proportionality includes 1) practicing a legitimate goal, 2) remaining within the limits required to achieve this goal, and 3) not placing an unreasonable constraint on the individual. If we specify this further to the proportionality principle within the context of AI technology use, we can also apply these three standards: 1) The first one refers to the "appropriateness or legitimacy" of the system, meaning the used technology should be appropriate when achieving the goal. 2) The second standards refer to the "necessity" of the method, meaning that the chosen technology should be necessary to achieve the goal. 3) Lastly,

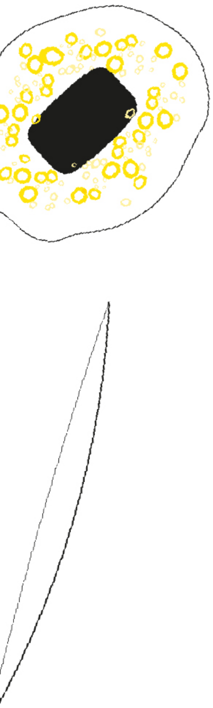


the method should not enforce any unnecessary constraint on any individual or affect any other stated (privacy) principle. This is described as proportionality “stricto sensu.” To summarize, this means that the content and form of technologies used should not go beyond what is necessary to achieve the intended goals (Karliuk, 2022). Altogether, the independent variable refers to how the proportionality principle is described and integrated within the EU regulations and acts and how effectively it safeguards privacy rights.

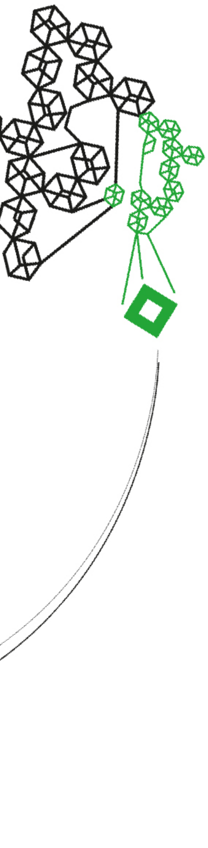
Next, the first dependent variable, **2) privacy rights of migrants** will be explained. Within the ECHR, privacy is stated, in the broader context, as a human fundamental right and refers to the right to have an anonymous, private life while having control of your own personal information, choices, and autonomy (European Data Protection Supervisor, 2025). In particular, for migrants, these rights are also applicable as stated in the conventions of the EU, since these rights are relevant to every individual regardless of their origin, status, country, etc. (Rehman, 2022). To specify, it refers to providing migrants the right to privacy by granting them control over how their data is collected and used (Migration Data Portal, 2022). There is no clear definition of how to describe privacy in the context of migrants. This can also be seen in academic literature since the institutions or organizations, when describing the privacy rights of migrants, refer to the general meaning of privacy as stated in the conventions. The attributes and how the concept will be measured within this research will be described in the Operationalization chapter. In addition, it should be clarified what is understood as personal data privacy as it is often understood as data protection. The privacy of personal data refers to how the personal data is being processed, and protection refers to how to store and protect the processed data (Emon, 2024). This research will focus on personal data processing, meaning collecting, storing, sharing, and transforming personal data into meaningful output that can be used by the algorithms of AI technologies (Mahendra, 2024).



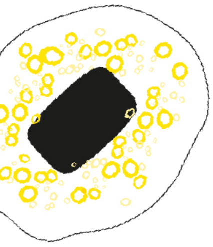
The second dependent variable, **3) relevant organizational expectations** will be explained. The variable should be split into two to understand the meaning of this concept in the context of this research. The relevant organizations in this context refer to public governmental and humanitarian/ NGOs organizations that operate within the migration and border control sector. These organizations are relevant since they are considering implementing (AI) technologies and are interested in what risks are involved regarding proportionality coverage when considering and implementing technological (AI) systems at border systems. Expectations refer in this context to what extent these organizations experience conducting a proportionality assessment as



a challenge and what expectations exist for clearer guidelines for the development of proportionality guidelines. Moreover, what expectations exist regarding how the inclusion of proportionality could potentially harm the privacy rights of migrants. It is also important to investigate if the relevant organizations understand what is required in terms of proportionality, privacy, and personal data processing, following European acts and regulations. The attributes of the relevant public and humanitarian organizations will include the legal structure and mandate, the authority to carry out policies (*Government mandate*, 2024), the mission and objectives of the organization, and the level of contribution in governance regarding AI policies. These dimensions will define and differentiate the public governmental organizations being studied.

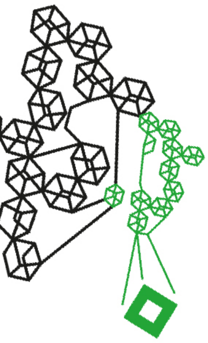


4. Case study: EU border management

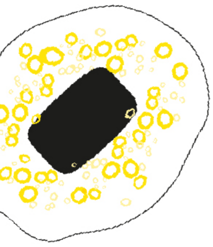


This section will describe the background and relevant reasons for the chosen case study: EU border management integrating AI technologies.

The Schengen Agreement was established in 1990, followed by the foundation of the Schengen Area five years later. The Schengen Area enables all travelers to cross internal borders without border checks within the EU. In addition to this, the MS agreed on a unified visa policy and codified police and judicial cooperation (European Court of Auditors). Consequently, the Schengen area established EU border management, which is mostly based on the Schengen Borders Code from 2006 (Andreou, 2023). Border checks occur at all of Europe's access points, such as ports and airports, but they also include the following procedures and practices, which are progressively being integrated into the EU MS bureaucratic systems regarding border controls. It can be seen as monitoring, registering, and cross-referencing people coming in and leaving the EU borders (Dijstelbloem & Broeders, 2014). However, since the migrant crisis in 2015, certain MS have experienced an unexpected inflow of irregular migrant arrivals, accompanied by concerns about unauthorized overstays, cross-border terrorism, and criminal activities in neighboring regions (Lehtonen & Aalto, 2017). To manage all activities, the European Border and Coast Guard Agency, called Frontex, assists the MS in handling the EU's external border control and combating transnational crime. This institution was established in 2004 and was initially meant to help guide MS by providing technical expertise and support within its border management (Gandhi, 2024). Nowadays, Frontex serves as a hub for knowledge and intelligence sharing regarding border control actions (Frontex, n.d.), to secure a high level of internal security through fighting crime and threats across the borders (Migration and Home Affairs, n.d.). To enhance the speed of these processes and identify a large number of entering individuals, different technologies have been established over the years.

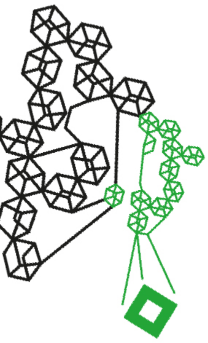


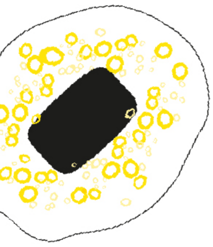
Internal border control is ensured through three automated systems, which all tackle different objectives. Firstly, the Schengen Information System (SIS) allows MS to share security and border management information, such as alerts of refusing entry to a country or criminal offenses. To do so, it is allowed to gather biometric data including fingerprints and facial photos. As each MS follows the same entry and short-stay visa regulations, another technology system has been developed, named the Visa Information System (VIS). This system is very useful because it allows countries to share (short) visa application information. This system also collects personal data such as fingerprints and facial images. The last system is called Eurodac, which is a



biometric database system that identifies fingerprint data of illegal migrants and asylum seekers at the location where they enter the EU. Consequently, it becomes clear which MS is responsible for the asylum application (Citizen Information, 2023; European Parliament, 2021). As can be read, these three systems collect a broad variety of personal data and functions utilized in border control and law enforcement (Orav & D'Alfonso, 2016). However, the European Commission (EC) noticed shortcomings in these systems due to more migratory complexity challenges (Orav & D'Alfonso, 2016) and MS needed higher resource commitments and infrastructural capacities to enable effective border control (Mahmutovic & Olson, 2020).

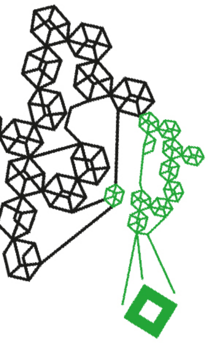
In response to these challenges, the European Commission introduced the Smart Borders Package in 2016, incorporating new centralized information systems designed to address multifaceted objectives (Orav & D'Alfonso, 2016). These systems enable MS to establish an information technology network for collecting, storing, verifying, comparing, and sharing diverse biometric data and characteristics obtained from migrants (Dijstelbloem & Broeders, 2014). Additionally, two new AI systems were introduced and are still in development for strengthening internal security and facilitating the detection of exceedances (Hirvonen, 2023). Those systems involve the Entry/Exit System (EES), which replaces passport stamps and provides a new form of entry, exit, and identity documents for all non-EU travelers, including travelers who do not require a Schengen visa for short visits, through biometric data such as fingerprints and face images (Jeandesboz, 2016). Additionally, the European Travel Information and Authorization System (ETIAS) executes an automatic risk assessment based on threat indicators and performs automatic cross-checks with other systems across the EU (Andreou, 2023). While these initiatives, mentioned by the European Commission (2011), aim to boost security and effectiveness, facilitate lawful travel, and mitigate the complexities arising from increased migratory flows, concerns and questions have emerged, making the potential risks of AI systems more apparent. Galdon Clavell (2017) raises pertinent issues regarding data privacy, potential discrimination of migrant groups, operational feasibility, and the substantial costs involved in implementing these technologies. There has been a considerable amount of discussion on the negative elements of AI technology employed in EU border management, such as the harm to data privacy and data protection. These concerns are valid because border control AI systems are not aligned with global data protection legislation (Andreou, 2023). Consequently, this results in an unequal distribution of advantages from technology growth because it favors the private sector as the primary driver, whereas governments employ these technologies to gain control



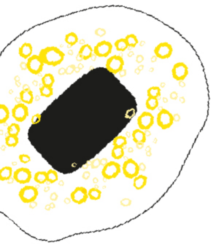


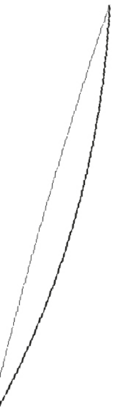
over migrant populations (Molnar, 2020). Furthermore, profiling or discrimination against certain vulnerable groups can occur through biased algorithms in AI systems. For example, Kieran et al. (2019) state that facial recognition algorithms trained on large datasets may lead to inaccuracies, such as misidentifying women as men or not recognizing them at all. This highlights, as stated by Andreou (2023), the risk of pre-defined risk indicators contributing to discriminatory or unlawful profiling, resulting in biased decisions. Additionally, migrants are usually unfamiliar with the scope and use of the data and what the actual purpose is. Consequently, they have no idea which privacy rights are violated (Hendow et al., 2015).

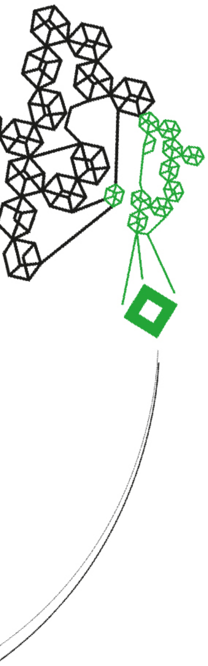
In response to these concerns, the EU has established certain acts and regulations, of which they recently introduced the Act to Govern Artificial Intelligence (the EU AI Act). This act describes the main regulations governing AI technologies nowadays. According to Molnar (2023), the EU AI Act has the potential to provide a strong regulation that protects the privacy rights of the most vulnerable groups, including migrants. However, it does not adequately address the risks associated with proportionality infringements, since it does not classify which rights should be outbalanced against the use of certain AI systems (Brouwer, 2024). This is making it harder to ensure that these principles are protected in practice. In addition, the General Data Protection Regulation (GDPR) has been in place since 2016, which is the world's biggest privacy and security law, also describing how personal data should be protected when crossing the (EU) borders (European Council, 2024). The GDPR has incorporated the principle of proportionality into its framework, however, in a non-understandable manner. This is because the GDPR describes the term proportionality in numerous ways, each time with different meanings or purposes, making it hard to understand exactly what is meant by the concept. In addition, it is unknown how to exactly assess the proportionality since this is not described in the GDPR enough (Kloza & Drechsler, 2020). In this context, the implementation of risk assessments assessing (AI) technologies and algorithms is becoming significantly crucial. The two established EU risk assessments are the Fundamental Rights Impact Assessment (FRIA) and the Data Protection Impact Assessment (DPIA). The FRIA is part of the EU AI Act, which obligates *only* AI technologies ranked as a high-risk system to conduct this assessment to identify the impacts the system has on individuals' fundamental rights, of which privacy is one of these rights (Rintamäki & Pandit, 2024). Furthermore, the DPIA is part of the General Data Protection Regulation and focuses on assessing breaches on privacy breaches, by categorizing activities of technologies that are expected to result in high risks, and therefore harming privacy rights (Rintamäki et al., 2023). As can be seen, (AI) technologies that will control personal data will

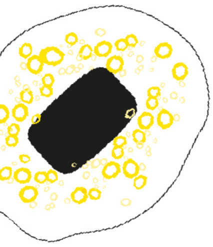


fall under both EU regulations, causing the risk category to depend on the different regulations and the MS involved. Consequently, this results in uncertainty about how to assess risks associated with privacy and personal data processing, especially how this data will be processed proportionately (Rintamäki et al., 2023).









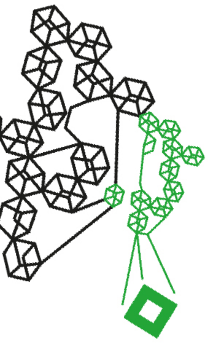
5. Methodology

5.1 Research design

To answer the research questions, multiple research methods will be used. These methods will be discussed per research question.

RQ 1: How is the proportionality principle embedded within the EU regulatory framework?

To answer the first research question, the thesis will conduct desk research, using qualitative secondary data from EU governmental reports and regulations including the EU AI Act and the GDPR. Desk research will help provide an overview of the current available knowledge on the inclusion of proportionality within these EU regulations (McCombes, 2023). In this research, the literature studied will be analyzed through content analysis, which entails examining the key themes within the literature to understand what most common themes regarding the inclusion of proportionality standards integrated into the regulations are (Luo, 2023). Understanding these themes will give significant insights into which issues are commonly discussed and which are underexplored, allowing the identification of potential trends that could help answer the research question. To conduct a complete content analysis, this study will specify particular units of analysis and define categories (or codes) for successful data organization and interpretation. By categorizing the content, the study hopes to find trends, gaps, and relationships within the material, resulting in a more comprehensive understanding of the subject matter.



RQ 2: What are the gaps regarding the proportionality inclusion within the EU regulatory framework compared to the practical implementation?

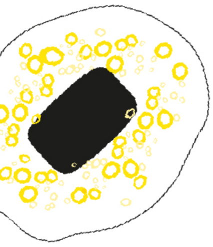
The second research question will be answered through first-hand and second-hand data. The second-hand data is established through desk research, obtaining qualitative secondary data from scientific reports, academic articles, opinion pieces, and reports from public organizations within the EU. The data helps identify the gaps (what should be done according to EU regulations versus what is done in practice) regarding the implementation of proportionality standards. To analyze the data content analysis is conducted to identify the most frequent themes (gaps), which derive from the literature, to investigate if there is any pattern within these themes.

In addition, this question will be answered through first-hand data, obtained from structured open-ended interviews with public organizations and privacy experts. Structured open-ended interviews allow for pre-established scripted interview questions, however, the respondent can give detailed answers while there is flexibility in the answers that will be given. This creates an in-depth understanding of the answers given (Thibodeaux, 2016). The respondents will be sampled through convenience sampling, which means finding respondents when the time and resources are limited. These respondents will be selected based on their accessibility and willingness to participate; due to the restricted time in which the thesis will be created and the confidentiality measures the thesis might have to take into account (Abbas, 2024). This way of sampling will produce multiple viewpoints and experiences from diverse relevant respondents. To create a comprehensive answer to the question, two groups of respondents will be interviewed. The relevant organizations that will be interviewed are public and governmental organizations within the migration sector. The privacy experts are experts within the Ernst & Young BV, who have work experience within the privacy and AI sector and have had hands-on practical experience with clients regarding the compliance and implementation of proportionality standards. An overview of the number of respondents per respondent group and the position within the organization applicable to this research, can be found in the table below.

Table 1: Overview of respondents

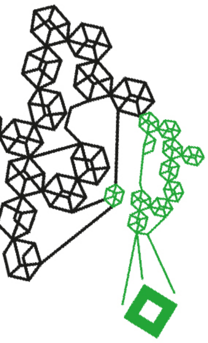
Type of respondent group	Number of respondents	Position in organization
Public governmental	4	• Information & Technology Board • Coordinator Privacy Office • Legal Counsel Privacy • Privacy Officer
Privacy experts	3	• Privacy Officer(s) • Chief Information Security Officer
Humanitarian/NGO’s	1	• Researcher & Journalist

The interviews will try to identify what is happening right now and they will try to answer what should be happening to safeguard privacy rights when using technologies at the borders. In this way, the gaps will be identified regarding the proportionality principle covered within the EU regulatory framework and the practical implementation within organizations.



RQ 3: Do the relevant public and humanitarian organizations' expectations align with the EU regulatory framework?

To conduct a more comprehensive understanding of the expectations regarding proportionality, structured open-ended interviews will again be held with the same public organizations that are willing to cooperate. These organizations can explain their expectations regarding the guidelines they seem to find essential for complying with the proportionality standards embedded in the EU regulatory framework. In addition to this, interviews will be held with humanitarian organizations or NGOs that are opting for the privacy rights of migrants. They will be asked questions regarding privacy rights infringements when personal data is collected/processed by AI technologies. For each respondent group, different questions were established. These insights can help identify the improvements necessary to enhance proportionality implementation in practice. Due to the time constraints, there will be one interview with each organization. However, when there is a low response of respondents within the human rights organizations sector, the findings will be strengthened with literature (written by human rights organizations). Since both sub-research questions 2 and 3 will be analyzed through structured open-ended interviews, some ethical assurances should be considered. Therefore, the names and details of the respondents will be treated confidentially and will be anonymized. In addition, the interview questions will be sent in advance, so that the respondent is aware of the structure and the expected questions.



RQ 4: What guidelines are necessary to enhance proportionality implementation when using (AI) technologies to protect privacy rights effectively?

To answer the last research question, desk research will be conducted, obtaining and examining qualitative secondary data. This includes analyzing earlier developed risk assessments that are (trying) to assess proportionality and associated risks within (AI) technologies and investigating to what extent these assessments are useful in safeguarding and assessing proportionality. In addition, the interviews held with respondents (regarding the gaps and views on proportionality) will help identify certain guidelines or create advice that will try to fill these identified gaps. Consequently, the desk research will help identify fitting guidelines, for example, by reviewing best practices in other sectors.

5.2 Operationalization

The research will examine to what extent and how the EU regulatory framework has included the proportionality standards and how these are implemented and understood in practice. To measure the inclusion of the proportionality standards within the regulations, it is essential to understand the criteria that can measure this inclusion of proportionality. The measurement of proportionality is based on the Amnesty International (2024) report which supports the rights of migrants while using technologies. Amnesty created a four-criterion test, based on the EU regulations and acts, to assess whether the principles of proportionality are incorporated when developing and applying AI technologies. The criteria also intertwine with the standards by the author Karliuk (2022), who explained proportionality within the AI context, which can be found in the Conceptualization chapter. The criteria consist of the legitimacy, the appropriateness, the necessity, and the proportionality in stricto sensu of the technology used. These criteria will be explained by their meaning within the table below.

Table 2: Criteria Proportionality

Criteria	Meaning
Legitimacy	The used technology should be in line and prescribed within the law.
Appropriateness	The used technology should be appropriate when achieving the goal.
Necessity	The used technology should be strictly necessary to achieve the goal (e.g. protect public security/order).
Stricto sensu	The used technology should not enforce any unnecessary constrain on any individual or affect any other stated (privacy) principle (e.g. discriminatory practices)

(Karliuk, 2022; Amnesty International, 2024)

To examine the variable privacy rights of migrants, the Organization for Economic Cooperation and Development (OECD) has created eight criteria on how to govern the protection of privacy concerning personal data processing. These eight criteria involve accountability, purpose specification, openness, collection limitation, data quality, use limitation, individual participation, and security safeguards (Organization of Economic Cooperation and Developments, 2013). The criteria and their meanings will be explained in the table below:

Table 3: Criteria Privacy Rights

Criteria	Meaning
Accountability	The person that is in control of the personal data should be accountable for complying to the criteria below, by taking measures when necessary.
Purpose specification	• The reasons for collecting personal data must be clearly defined • Any following collecting of personal data should be restricted to fulfill the purpose • Any change of purpose should be communicated directly.
Openness	All information regarding collecting, using and storing data should be openly and readable available to anyone.
Collection limitation	Data collection should be limited, appropriate and with consent of the data subject.
Data quality	Personal data that is collected must be only applicable to the intended purpose, necessary and accurate.
Use limitation	All personal data should be available, if not it should agree with • Consent of data subject • Authority of law
Participation	Individuals must be able to obtain the personal data and if not have the right to fight this denial.
Security	The personal data should be protected against loss, unauthorized access and use.

(Organization of Economic Cooperation and Developments, 2013)

5.3 Data Collection

Within this section, the data that has been collected and examined for the research are described below. To measure the variables, the researcher only uses qualitative data, which derives from primary and secondary data sources. The qualitative data will address all sub-questions by examining key elements of the proportionality standards within the EU regulatory framework, identifying gaps when implementing the principle, and assessing its impact on the protection of privacy rights. The primary data stems from interviews with three different kinds of respondent groups. The first respondent group is relevant public governmental organizations, which are asked about the (AI) technologies used or being considered, which personal data is being processed, how these organizations understand and implement proportionality, and what guidelines they find necessary in order to enhance understanding and implementation of the principle. The second group of respondents are privacy experts, who will try to give insight into their knowledge and experience with the implementation of proportionality standards in practice. The aim is to gain information about what best practices or guidelines could be in order to enhance this. The last respondent group is civil society/NGO's which are asked about the rights that might be violated of migrants when not implementing proportionality effectively.

The second-hand data is obtained from earlier academic research, relevant governmental documentation, the GDPR, the EU AI Act, and policy analysis.

Due to the gathering of primary data, some ethical considerations should be included. The obtained primary data could have sensitive information that should ensure confidentiality. To do so, a few measures are in place. The names and details of the respondents will be treated confidentially and will be anonymized within this research. This means that no names/details of the respondents are mentioned within the thesis, consequently, when referring to interviewed organizations, the thesis will use a general term (relevant public governmental organizations, privacy experts, NGOs). Also, no exact quotes or answers derived from the interviews will be included in the research, but the answer to each sub-question will be generalized in order to prevent traceability to an organization. The interview transcriptions are destroyed at the end of the study, and a draft of the data used within this research can be sent to the respondent. In addition, the interview questions were sent in advance, so that the respondent was aware of the structure and the expected questions. An overview of the data collection methods is described within the table below.

Table 4: Data collection matrix

Theoretical concept	Variable	Measurement	Data Collection
Regulatory framework European Union	Proportionality	What is the inclusion of the proportionality principle within the EU regulatory framework?	• EU AI Act • GDPR • EU governmental reports on proportionality measures
Relevant public organizations expectation	GAPS proportionality implementation	What are the gaps regarding the inclusion of proportionality compared to the	Structured open-ended interviews with the relevant public organizations, privacy experts and civil society organizations/ NGOs.

		practical implementation?	
	Privacy rights	To what extent are the privacy rights of migrants protected when proportionality is not implemented completely?	• EU AI Act • GDPR • Reports and research from public (human rights) organizations • Structured open-ended interviews with relevant respondents

5.4 Data Analysis

This section will explain how the obtained data is analyzed in order to give answers to the research questions. For a systemic analysis of the collected data, such as literature reviews and interview transcripts, a program like Atlas.ti will be used. The data will be coded using thematic analysis to thoroughly review and identify relevant trends. For the structured open-ended interviews, an inductive thematic analysis technique is executed, which means that codes will be created after the interviews are completed. As a result, these codes were developed later in the study process, allowing them to emerge naturally from the acquired data (Medelyan, 2024). For the desk research, a deductive thematic analysis technique will be used, which means that the codes will be created beforehand to identify themes. This entails searching for common themes regarding key components of proportionality and privacy criteria within the EU regulatory framework, searching for gaps, and implementing measures. The coding schemes for sub-questions 1 and 2 are described below. The coding scheme of the conducted interviews is described in Appendix 1.

Figure 4: Coding scheme sub-question 1

Main Code	Sub-code	Open code
Inclusion of Proportionality	Legitimacy	The used technology should be in line and prescribed within the law.
	Appropriateness	The used technology should be appropriate when achieving the goal.
	Necessity	The used technology should be strictly necessary to achieve the goal (e.g. protect public security/order).
	Stricto sensu	The used technology should not enforce any unnecessary constrain on any individual or affect any

		other stated (privacy) principle (e.g. discriminatory practices).

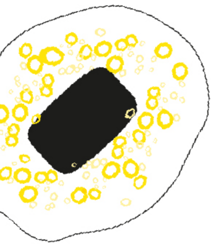
Figure 5: Coding scheme sub-question 2

Main Code	Sub-code	Open code
Privacy	Accountability	The person that is in control of the personal data should be accountable for complying to the criteria below, by taking measures when necessary.
	Purpose Specification	Clear purpose definition, limited data use, and transparent communication of any changes.
	Openness	All collection, usage and storing information should be available to the public.
	Collection Limitation	Data collection should be limited and with consent of the data subject.
	Data Quality	Personal data that is collected must be only applicable to the intended purpose, necessary and accurate.
	Use Limitation	Data access must be lawful, based on informed consent or legal authority.
	Participation	Individuals must be able to obtain the personal data and if not have the right to fight this denial.
	Security	The personal data should be protected against loss, unauthorized access and use.

5.5 Validity and reliability

The operationalization of this research takes the insurance of validity and reliability into account. Validity can be measured in multiple forms, but for this research, content validity is applicable. Content validity refers to how well and comprehensively the instruments will cover all relevant parts of the concept that are aimed to be measured (Nikolopoulou, 2022). The content validity is ensured by using the different criteria from Amnesty International (2024), Karliuk (2022), and the OECD (2013), which are all developed by experts in the field who have done similar research before on the different sub-questions. In addition, validity will be ensured because of triangulation, using multiple data sources to answer every sub-question. Triangulation is also applied to the interviews, which use three different types of respondents. These respondents all have different expertise and backgrounds, enhancing the validity and representativeness of the respondents. Reliability should also be considered, which refers to the extent the results of the research can be reproduced under the same conditions (Middleton, 2023). The reliability will be ensured by documenting how the literature is analyzed and how the interviews are conducted, allowing other researchers to replicate the study. Most academic research and sources are retrieved from Google Scholar and Scopus.

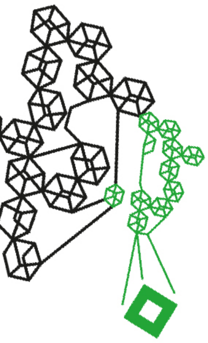
6. Results



Within this chapter, the findings will be described to answer the main research question and sub-research questions. The chapter will begin by outlining the legal foundations of the EU regulatory framework governing (AI) technologies, particularly in the context of safeguarding the proportionality principle. Following this, an analysis of the gaps regarding the proportionality inclusion compared to the practical implementation will be provided. Next, the findings from the interviews will be presented, offering insights into the expectations of relevant public organizations, knowledge of privacy experts, and views of humanitarian organizations. Finally, the chapter will discuss the potential guidelines that could be developed to effectively enhance proportionality implementation in practice. These guidelines will (try to) address the identified gaps and issues, offering suggestions for strengthening the regulatory processes.

6.1 Contextual findings

Before describing the outcomes per research question, the interviews with the respondents revealed a finding that is relevant to discuss to gain a better understanding of the research problem, the context of the problem, and the results. The theoretical framework of this research highlighted the growing use of AI systems in the border management practices of the EU to enhance speed and effectiveness while (potentially) breaching fundamental rights of migrants. However, interviews with respondents revealed that most of these governmental organizations are currently implementing or in the early process of utilizing these AI systems[1]. As one of the respondents, positioned as Coordinator Privacy Office, stated: ***"There is very little AI or high risk in the sense that we see AI in the world as advanced tooling that contains training data or is tested with. There is virtually no such thing within our organization. According to the AI Act and the definition as it is described in it, there is simply very little."***



Another example stated by a member of the Information and Technology Board: ***"Looking at the definition of AI as it is stated in the AI Act, the organization isn't using these systems at the moment."***

Nowadays, these organizations still primarily rely on automated or technological systems with a human oversight aspect within the decision-making process. Systems mentioned in the theory, such as the ETIAS, VIS, SIS, and EES, are still automated systems without AI components, though they are incorporating AI in these systems in the upcoming year. Although predictive AI

[1] *Interview code A-24, A-25, B-26 and A27*

systems are extensively discussed in the literature, the findings from interviews indicate that most public/governmental organizations are still in the early stages of piloting or considering the implementation of such AI systems. Frontex has begun to explore and carefully pilot AI in specific analytical and surveillance roles, such as drone image identification and migration forecasting. Yet, they do not incorporate AI in their decision-making processes (McCormick et al., 2025). Despite this gap between theory and practice, this research remains important. The principle of proportionality, which is central to this study, applies to AI systems but also to other technologically/automated systems that process personal data. Furthermore, as the EU AI Act enters its implementation phase, understanding how proportionality is described and could be implemented according to the EU AI Act becomes increasingly important.

6.2 Legal embedding of proportionality

To answer the first sub-question: ***How is the proportionality principle embedded within the EU regulatory framework?***, the most relevant EU legislation governing personal data processing has been examined. In particular, these regulations have established a legal framework for the processing and protection of personal data while developing and utilizing (AI) technologies. First, there will be an explanation of the legal foundation regarding the proportionality standards within the EU regulatory framework. In addition, there will be a short examination of the proportionality inclusion within the associated risk assessments.

The GDPR and the EU AI Act are subject to the primary EU law principles, such as the TEU and the CFR. These primary EU laws do cover the principle of proportionality in a broader sense, and it is essential to identify how and to what extent these principles are stated to understand the derivation and inclusion of the principle in the GDPR and AI Act. Table 3 will show the primary proportionality principles as stated in the CFR and TEU.

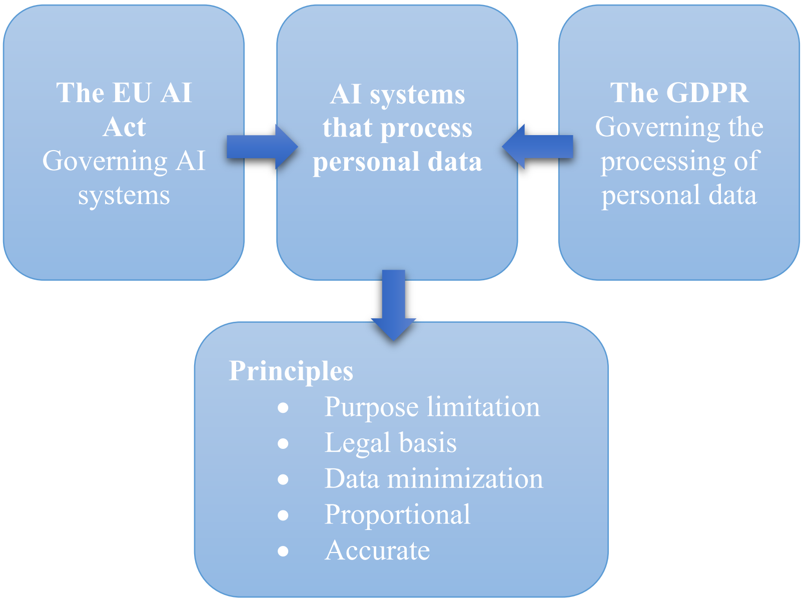
Table 5: Proportionality (broad definition) in primary EU legislation

Regulation	Article	Definition as stated
TEU (The Treaty of European Union, 2012)	Article 5	*“The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. National Parliaments ensure compliance with the principle of subsidiarity in accordance with the procedure set out in that Protocol.*

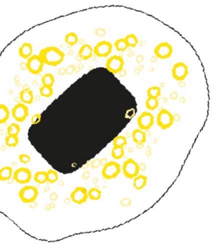
		Under the ***principle of proportionality****, the content and form of Union action* ***shall not exceed what is necessary to achieve the objectives*** *of the Treaties."*
CFR (Charter of Fundamental Rights of the European Union, 2000)	Article 52.1	*"Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the* ***principle of proportionality*****, *limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others****."*

Now that the primary EU legislation has been identified, it is essential to understand why the EU AI Act and the GDPR were chosen to be analyzed for this research. Figure 4, created by the author, however, derived from the authors Gonzalez Riedel and Idema (2024), shows the application of both the EU AI Act and the GDPR within the field of technology usage on individuals. This figure explains the most important alignments between the two regulations and the differences that appear. In addition, it shows the principles that should apply and be covered within both regulations.

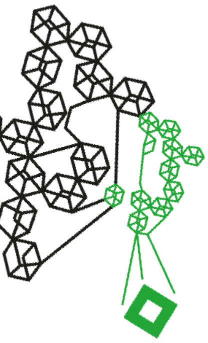
Figure 6: Intersection of the EU AI Act and the GDPR principles



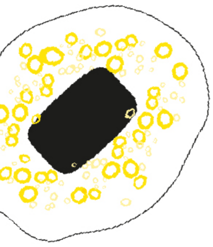
6.2.1 Legal Framework GDPR



One of the most relevant legislations covering and explaining privacy standards is the GDPR, with a specific focus on protecting individuals against the processing of personal data and the movement of this data across different MS. All the information and articles stated within this section are retrieved from the official GDPR (2016) document and will be cited as stated in this regulation. The analysis of the inclusion of the proportionality principle (the legal base) is based on the four established criteria by Karliuk (2022) and Amnesty International (2024) as described in Table 1 within this research. These criteria include the inclusion of proportionality as stricto sensu, necessity, appropriateness, and legitimacy. To what extent and how these criteria are included within the GDPR is shown in the very detail in Appendix 2. Only the most comprehensive and relevant parts, encompassing the proportionality criteria, within the regulation are described within the appendix.



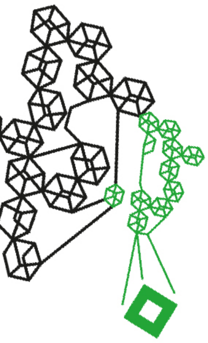
Although the principle of proportionality is technically embedded within the GDPR, its normative existence does not necessarily ensure practical appropriateness. Many articles, such as Article 5.1(c), 6.1(f), 23, and legal provisions 39, 47, and 170, specifically state that "***data processing operations must be suitable, necessary, and proportionate given their objectives"*** as shown in Appendix 2. All of these references indicate a fundamental base to the principle of proportionality based on the primary EU legal principles like those in the CFR and the TEU. However, upon closer examination of the GDPR, it becomes clear that the GDPR lacks guidance on how proportionality should be measured and implemented in practical and concrete terms. Even though proportionality is often mentioned, particularly when discussing lawfulness, legitimacy, and necessity, it remains a primarily theoretical concept within the legal framework of the GDPR. It does not specify what thresholds or criteria should be applied to determine proportionality in particular situations. This is also evident in the literature; often, controllers are not qualified to perform a complex and specialized legal analysis. Under the Data Protection Directive, dealing with proportionality has already caused challenges, particularly when controllers were required to provide evidence of legitimate interest in processing (Kloza & Drechsler, 2024). The entire objective of the proportionality principle could be compromised by the lack of precise interpretive or procedural standards, especially in situations when individual rights may be restricted for national security or public interest reasons (which is most of the time the case in the migration sector). Legal provision 73 and Article 23(b-c) permit such exclusions as long as they are ***"necessary and proportionate"*** but the regulation provides little specific guidance on how these evaluations should be carried out or assessed. The implementation of



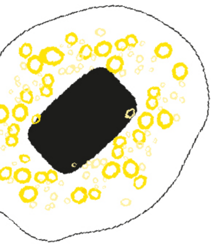
proportionality may therefore be largely left up to the professional judgment of national authorities or courts, which could lead to legal ambiguity and even inconsistency across MS. In conclusion, while proportionality is embedded in the GDPR, it remains formal and very general rather than practical and detailed. Without explicit operational guidelines or procedures for assessment, the concept may be more symbolic than functional in data protection practices.

6.2.2 Legal Framework EU AI Act

Since 2021, the EU has been working on establishing its first EU AI regulation, which focuses on governing the implementation and usage of AI technologies by introducing a risk-based categorization of AI systems. Since that moment, the law has been revised, and in 2024, the EU AI Act entered its force. All the information within this section is retrieved from the official EU AI Act (2024) document. Also, here, the EU AI Act is analyzed through the four criteria of proportionality as described in Table 1. To what extent and how these criteria are included within the EU AI Act is shown in the very detail in Appendix 3. Only the most comprehensive and relevant parts, encompassing the proportionality criteria, within the regulation are described within the appendix.



Analyzing the EU AI Act shows us that, formally, the principle of proportionality is embedded within the regulation. As described in Appendix 3, proportionality, along with the pre-established criteria, is mentioned in several articles, including Articles 5.3, 13, 36.7(e), 44.3, 88.2, and legal provisions 33, 34, and 176. These regulations jointly define that AI systems, particularly high-risk or biometric identification systems, ***must be necessary and not beyond what is necessary for their intended purposes.*** Also, within the EU AI Act, the regulation makes exceptions regarding proportionality for public interests as stated in legal provision 33: *"The use of those systems for the purpose of law enforcement should therefore be prohibited, except in exhaustively listed and narrowly defined situations,* ***where the use is strictly necessary to achieve a substantial public interest****, the importance of which outweighs the risks…"*. Managing migration issues and controlling borders can be identified as substantial public interests, creating an opportunity to not comply with proportionality standards. In addition, the EU AI Act does not adequately provide guidance on how to assess this substantial public interest or the risks that should outweigh each other and thus justify the intrusions on persons' rights. In addition, Article 14 of the EU AI Act requires that high-risk AI systems be monitored by at least two people to ensure that decisions are fair and responsible. However, sub-paragraph 5 offers an exception for systems used in migration and border control, stating that this criterion does not apply if its application would be "disproportionate". More importantly, the regulation does not specify what

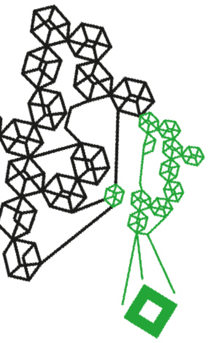


that means or what contradicting interests would justify such an exception. This is concerning because these are sensitive sectors where human supervision is critical to safeguard people's privacy rights. Without human supervision, migrants may be affected by incorrect or unfair automated decisions, with limited opportunity to appeal against them, which violates Article 47 of the CFR (Pina, 2025). As a result, while the EU AI Act defines proportionality as a guiding legal concept, its current definition lacks the normative clarity and operational guidelines or requirements needed for effective implementation. Similarly, with the GDPR, the inclusion of proportionality in the EU AI Act appears to be more symbolic than functionally implementable.

6.2.3 Risk assessments

The tables in Appendices 2 and 3 present an analysis of the GDPR and the EU AI Act in relation to the inclusion of the proportionality principle, assessed through the 4 pre-established criteria. For both regulations, risk assessments are mandatory, therefore, it is beneficial to examine the inclusion of proportionality within these assessments.

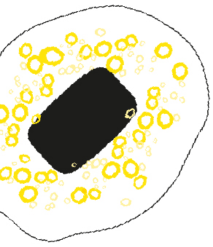
Both regulations have tried to create comprehensive regulations to govern data collecting and processing when using (AI) technologies and therefore legally safeguarding the rights of the individual. They both include the principle of proportionality as stated within the primary EU legislation and elaborate on these principles by using terminology such as “data minimalization” and “does not go beyond what is necessary”. In addition to this, both regulations obliges providers and users to assess their technologies through assessments. The AI Act requires, in addition to their risk-based approach, a Fundamental Rights Impact Assessment (FRIA) for high-risk AI systems (The EU AI Act, 2024) and the GDPR requires a DPIA for technologies that process high-risk personal data (GDPR, 2016).



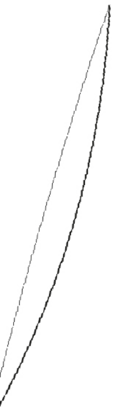
However, within these assessments, the principle of proportionality is covered in the same (subjective and formal) manner as within the regulations. As stated within these risk assessments:

- Within the FRIA**:** ***“Are the objectives sufficiently weighty to justify affecting fundamental rights?”*** *(Ministry of the Interior and Kingdom Relations, 2022).*
- Within the DPIA, “*First and foremost, the processing must be proportional. This concerns the question of effectiveness and proportionality.* ***If the processing of the data does not achieve the intended purpose, or if this is highly unlikely, the processing is not easily proportional****. The second element of the proportionality test concerns the*

> *balance.* ***The legitimate objective being pursued must be in proportion to the fact that personal data must be processed for this purpose****." (NOREA DPIA, 2020).*



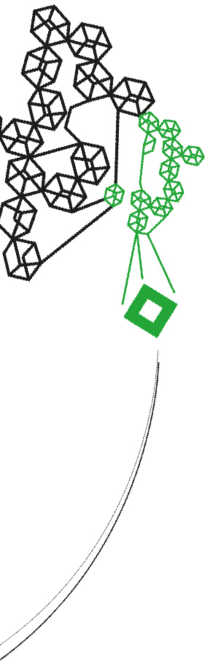
Although this looks promising in effectively tackling the risks that arise from using (AI) technology, some weaknesses should be addressed. Both regulations refer to relevant and adequate systems that should be used to process specific data. The "relevant" and "adequate" concepts of this explanation remain vague and normative. When is it relevant to obtain personal data? And when is the obtained personal data adequate? Due to the different stakeholders involved, this meaning could have different interpretations and therefore, different outcomes. This is also the case with the terms referring to "necessary" and "appropriate" data usage and processing. For one organization, data processing is necessary for a certain goal, while for another organization, this data processing is not necessary to achieve the same goal. In addition to the appropriateness term, within the EU AI Act, the term " appropriateness" is mostly used in the context of taking measures by the EU. In this context, it means that the Commission of the EU should be taking appropriate measures to tackle risks regarding data protection. This does not require using or developing appropriate (AI) technologies, methods, or processing of personal data.

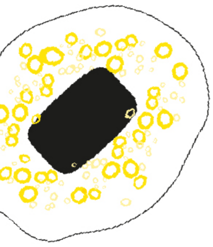


To conclude and answer the sub-question on how proportionality is embedded within the regulatory framework, a hypothesis has been established before examining the data.

H1: The principle of proportionality is formally included within the EU regulatory framework but is missing regulatory guidance for practical implementation.

The analysis has shown that the hypothesis can be confirmed, since it is evident that the principle of proportionality, according to the four established criteria, is embedded in all (primary) regulations. Despite its formal presence, the clarity and practical measurability of proportionality remains problematic. The different ways in which proportionality has been embedded across these regulations show a lack of consensus and guidance on the principle (Kloza & Drechsler, 2024). There are no clear guidelines embedded within the regulations or risk assessments that explain or describe how proportionality should be measured in practice and what criteria could be applied to do so.



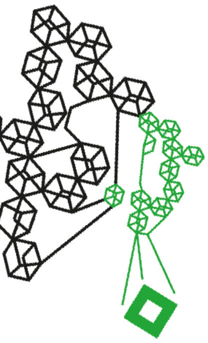


6.3 Practical implementation

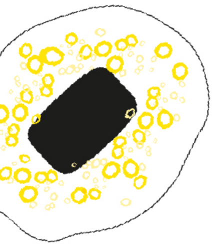
The inclusion of the proportionality principle within the relevant EU regulations has been examined in the previous section. Within this section, the research tries to answer the sub-question: ***What are the gaps regarding the proportionality inclusion within the EU regulatory framework compared to the practical implementation?.*** To do so, literature has been examined and interviews have been conducted with public/governmental organizations and privacy experts to understand what should be happening according to the EU regulatory framework and what is actually happening in practice, identifying the gaps.

Legal (in)compliance

The first finding from the interviews is that organizations act in accordance with what is formally described within the EU regulatory framework[2]. Their primary objective is to comply with these laws and consequently stay out of legal complications. While this appears to be positive, it could lead to a so-called "checkbox approach". This means that the organizations rely on compliance-focused execution, trying to tick the boxes on paper, however, providing insufficient protection in practice (Thiel, 2022). As the interviews and literature reveal, the principle of proportionality is very vague and subjectively described within the regulatory framework[3]. Employees within the organization often do not know how to interpret the principle and, consequently, are unable to execute it, as stated by a Coordinator Privacy Office: ***"It is still unclear how to assess a proportionality principle since people don't understand what is meant by the concept."*** Additionally, the broadness of the principle allows for a wider interpretation and increases the justification of data processing on legal grounds. This is evident in how the organizations frame proportionality in, for example, their DPIAs[4]. For instance, one member of the Legal Counsel Privacy mentioned that ***"Sometimes the problem for which the technology should be used is too little to be appropriate. Therefore, the organization tries to frame the problem bigger in order to justify the technology."*** Organizations appear to be compliant on paper, even when not always considering potential harms to privacy rights. This shows that a legal framework is sufficient, although it could potentially lead to "ticking the boxes" rather than looking further into the deeper ethical considerations. Following this, when the organizations were asked about complying with proportionality standards and how they operationalize these standards, they all



[2] *Interview code A- 11, A-12 and A-13*
[3] *Interview code B-18 and A-19*
[4] *Interview code A- 16*

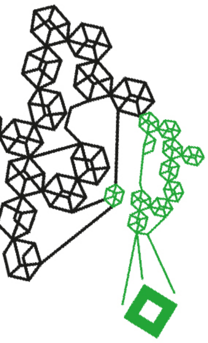


referred back to the execution of a DPIA as their primary mechanism to measure these standards. The DPIA is indeed a risk assessment that should be conducted when processing personal data with a high risk, yet noticeable practical issues were identified during the interviews that are relevant to discuss.

Data Privacy Impact Assessments

Within the GDPR, Article 35 requires that every organization conduct a DPIA before undertaking processing activities that are likely to pose a high risk to fundamental rights. This requirement has been established to mitigate privacy risks that could arise from processing personal data. As stated in Article 35.1 (GDPR, 2016): *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, **prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.** A single assessment may address a set of similar processing operations that present similar high risks."*

Within this DPIA, the principle of proportionality should also be examined when deploying a technological system: *"The assessment shall contain at least **an assessment** of the necessity and **proportionality** of the processing operations concerning the purposes"* (GDPR, 2016).

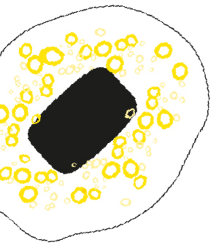


Based on interviews conducted with relevant public/governmental organizations and privacy experts, some problems occur related to the understanding and execution of a DPIA in practice. Looking at the execution of a DPIA when organizations consider implementing a technological system, it becomes clear that all respondents' organizations carry out a DPIA too late[5]. They often conduct a DPIA midway through [6], when the system is already operational, or even at the end, when the system is fully operational and thus already processing personal data. According to privacy experts, they also observe this issue in practice mentioning the following[7]: ***"The theory is, of course, someone wants to develop a system, the organization has to go through a compliance route and should do a DPIA in advance. Practice shows that this does not always happen."*** At this stage, the evaluation of whether the technological system may violate privacy

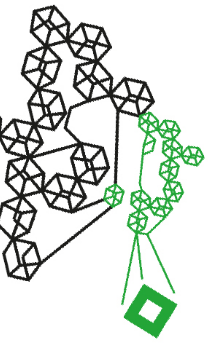
[5] *Interview code A-02, B-03, B-04, A-06 and B-08*

[6] *Interview code A-01*

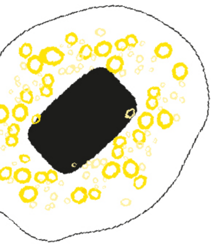
[7] *Interview code B-03*



rights is often biased[8], as organizations invest significant time and resources into developing the system. As one of the Privacy Experts explained:
“Organizations should conduct a DPIA in advance; otherwise, they risk investing excessively in the development process without fully understanding the privacy implications. If the DPIA is completed too late, it is frequently filled in with the bias of 'it's good this way,' which nearly assures organizational resistance and potential failure.” The tendency is thus to proceed with the system rather than halt deployment, even though it may potentially harm privacy rights. As a result, DPIAs tend not to be completed with full objectivity or accuracy, as previous investments in the system can influence the outcome. Furthermore, these organizations do not in practice comply with the GDPR, as stated in Article 35, since the DPIA should always be conducted before processing. As a result, the next practical issue arises. The interviews reveal that when assessing the DPIA in a later stage within the process, the risks that could harm privacy/fundamental rights will be accepted more quickly[9]. This is due to the already mentioned process in which the need to proceed with the systems outweighs the risks that may arise. Especially within the migration and border control sector, the respondents do acknowledge that sometimes risk acceptance is necessary to reach their goals, such as public safety. Remarkable is that a Privacy Officer of a governmental organization mentioned ***“Sometimes the organization discovers things being done in practice while if they had done the DPIA in advance, they would never have started the process of the system.”***
Additionally, a Privacy Expert mentioned: ***“Ultimately, the purpose is to determine whether the chosen systems are consistent with the stated objectives. The guiding idea is to avoid utilizing technologies or processes that do not serve a clear purpose, though in practice, there may be exceptions.”*** These actions could lead to serious human rights infringements. Moreover, in some cases, the organizations accept these potential risks and describe them within the DPIA, explicitly stating that the regulator has failed to provide a clear legal basis for certain operations[10]. As stated by a member of the Legal Counsel Privacy ***“In the DPIA you are not writing down that something isn’t proportional, but the organization describes that the policymakers have failed to provide a specific basis for these risks and do accept them.”*** By doing this, the responsibility and potential risks are shifted to a higher decision-making level.



[8] *Interview code B-04*
[9] *Interview code A-07, B-08 and A-09*
[10] *Interview code A-10*

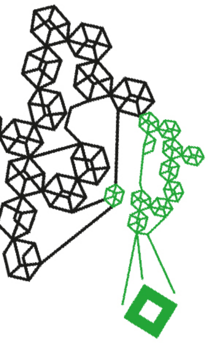


The EU AI Act in the migration context

As previously stated, both the GDPR and the EU AI Act have been assessed in terms of proportionality. It is particularly important to consider the wider scope of the EU AI Act, since it is evident from the interviews that the migration sector is complex to navigate.

The EU AI Act's scope is widespread, as it applies to any AI application and any user within the EU, regardless of their country of residence. The act focuses on four categories of systems that might pose risks to the privacy and fundamental rights of individuals. Banned systems are prohibited as they pose significant risks to fundamental rights and privacy (The EU AI Act, 2024). The high-risk systems are not prohibited, but they do have a lot of requirements to be deployed. As specified in Article 71 of the EU AU Act, high-risk systems should be reported in the EU database. However, in the field of migration and border control, there is an exception from public registration (Article 49.4 in the EU AI Act) and from releasing a description of the AI project generated (Article 59.1 in the EU AI Act). While this solution represents an approach that should ensure the secure use of AI, it adds to the already concerning ambiguity surrounding the use of AI in migration, obstructing public scrutiny and effective monitoring of the effects of these systems on the rights of migrants. (Pina, 2025). Moreover, and even concerning, is that the mentioned systems, such as ETIAS and SIS, do not have to comply with the EU AI Act till 2030, even when the goal is to make these systems operational in 2026 (Brouwer, 2024).

Additionally, the EU AI Act requires a FRIA to be executed when deploying high-risk AI systems. This assessment would be useful (not looking at how proportionality is embedded within this assessment), though the EU AI Act Article 27.1 describes that there are exceptions for high-risk AI systems intended to be used in the area listed in Annex 3, which includes the migration, asylum, and border control management sector. This means that governmental organizations do not have to execute a FRIA to deploy any AI system used in their border management. This is very concerning, since this is the only risk assessment required by the EU AI Act that could be performed to assess whether the system is proportional and safeguards fundamental and privacy rights of migrants.



Privacy teams

Based on the interviews, all respondents recognized that the principle of proportionality is a concept that is very important to consider when developing a technological (AI) system. As seen in the literature before, proportionality is widely embedded within the EU regulatory framework, yet it's subjective nature and broad interpretation creates that the organizations do not know how to precisely tackle the proportionality principle when executing a DPIA (leaving the FRIA out

since the relevant organizations do not use AI systems, yet). Derived from the interviews, it is evident that organizations often try to write proportionality in a way that favors them to continue with the technology[11]. Sometimes the problem for which the technology should be used is too small to be appropriate. Therefore, the organizations try to frame the problem in a bigger context in order to justify the technology. Moreover, nowadays, certain tools exist, such as ChatGPT, which can write the proportional way of deploying a technological system in such a way that will justify the technology and potential breaches to fundamental and privacy rights, which is very concerning. This means that organizations do not look at the ethical issues that may arise, just to be compliant within the DPIA or broader in the regulations.

To address legal and practical difficulties related to proportionality and other privacy obligations, most of the organizations have established privacy teams[12], which include Privacy Officers or Information Security Officers. Although this is a sufficient and necessary step, respondents acknowledge that these teams often lack the tools or guidance needed to understand and apply proportionality in practice. This could cause no further proceeding with the implementation of a technological system in the final stage, since the problem of proportionality is still being discussed internally until there is a clear solution to resolve it[13]. This is due to limited knowledge since, in the opinion of the organization, the topic is still relatively new. In addition, there is limited collaboration across organizations to share best practices regarding proportionality assessments, since it is a relatively new subject concerning technological (AI) systems. Although a proportionality assessment is mostly context and case-by-case specific, respondents agreed upon a framework or sector-specific guidance that could assist with proportionality embeddedness in practice.

Privacy criteria

Within the methodology section (Table 3 and Figure 5), some privacy criteria were established to examine which privacy rights are being violated when certain gaps exist in practice. One of these criteria is "use limitation", referring to all data activities and access to the data should be stated within the laws and should be in consent with the subject. Looking at the practical activities, it seems like the organizations do align with this criterion, because they act based on the laws and regulations. In addition, most of the organizations publicly state which data they are processing

[11] *Interview code A-16 and B-15*
[12] *Interview code A-20, A-21, B-22 and B-23*
[13] *Interview code A-17*

and what systems they use. It is unclear whether the processing is done with the subject's full agreement, as the majority of the subjects are migrants who are unaware of what privacy implies or what their other rights are. They also make this choice of consent under coercion, since they then get access to basic needs for example. This is concerning, since the consent is not given in agreement and most of the time it is unclear for these migrants what information is being processed (Temirov, 2025). In addition, as described before, the AI systems within the migration and border control sector do not need to comply with the publication regulation. Resulting in violating the privacy criteria of "openness", "transparency", and "purpose specification", since it is not clear what the reasons are for collecting the data, and any information regarding this is not available to the public. Also, organizations exaggerate problems in order to justify the use of technology, which undermines the clarity and limitations of the purpose of the technology. Furthermore, examining the criterion of "accountability" reveals that this is violated during the late execution of DPIAs and the shift towards higher decision-makers when accepting certain risks. This shows that accountability is shifted towards others at a higher level.

To conclude and address the sub-question regarding the practical gaps in the regulatory framework concerning proportionality, a hypothesis has been established before examining the data.

H2: There exist significant gaps between the proportionality inclusion within the EU regulatory framework and the practical implementation.

The analysis shows that the hypothesis can be confirmed since the data analysis and interviews have demonstrated that the practical implementation remains insufficient. While organizations operate in formal accordance with EU regulations and frequently base their data processing activities on legal grounds, this alignment does not always translate into effective privacy rights protections. This issue arises from the delayed execution of Data Protection Impact Assessments (DPIAs) when technological systems are already operational. Even though most organizations depend on this assessment to evaluate and ensure compliance with proportionality, there are still concerns and critical problems arising. One of these problems is the framing of proportionality in such a way that the technology is justified for its purpose, even when the problem isn't big enough. Additionally, the scope and exceptions of the EU AI Act for AI systems used in border management raise serious concerns. More importantly, the vagueness surrounding the lack of guidance for executing the proportionality principle creates significant practical gaps compared to the legal basis governing proportionality, resulting in the violation of multiple privacy criteria.

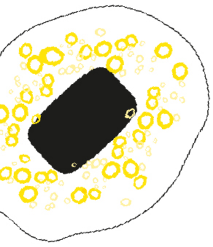
6.4 Relevant expectations

This chapter will answer the following sub-research question: ***Do the relevant public and humanitarian organizations' expectations align with the EU regulatory framework?.*** For this chapter, findings were derived from interviews conducted with relevant public governmental organizations and human rights organizations/NGOs, as well as literature written by these organizations and NGOs.

The findings from both the interviews and the literature review show an alignment between what is stated within the EU regulatory framework regarding proportionality and data protection measures and the relevant public expectations. However, this alignment differs between governmental organizations and human rights organizations. Evident from the interviews is that the public and governmental organizations think they do align and comply with the regulations. This is because most organizations attempt to comply with these regulations but often overlook further consideration of ethical implications. This does not mean these organizations do not consider ethical issues completely; it means that they just do what is asked of them instead of thinking outside the box. They expect that, as long as they comply with these regulations and assessments, they will meet the required proportionality standards, since they rely on these regulatory frameworks. The GDPR has been established with its primary goal to ensure privacy when processing data, whereas the EU AI Act was established to ensure a human-centric method for deploying AI systems. Consequently, this feeling of reliance on the regulations of organizations is indeed validated when they do meet the requirements mentioned. If the regulations stay vague and remain incomplete in regard to giving strict guidelines, organizations will act in accordance with what is concrete, familiar, or legally defensible. However, the interviewed organizations do recognize that it would be helpful to have additional guidelines to better understand what is exactly meant by proportionality, to describe the standards better in the future, within, for example, their DPIA or FRIA.

One of the expectations regarding a better understanding of proportionality is that the principle is frequently viewed as a principle standing on its own. Although this is true, it would be more competent to include the principle of necessity and subsidiarity when assessing and determining proportionality[14]. As seen in the literature and the pre-established criteria of proportionality (Table 2 and Figure 4), necessity is already a criterion, meaning that the technology being

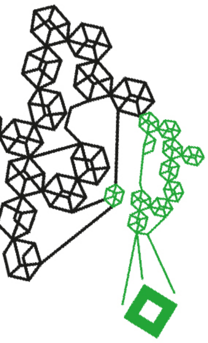
[14] *Interview code A-30*



considered needs to be strictly necessary to achieve the goal (Karliuk, 2022; Amnesty International, 2024). These criteria do not mention the principle of subsidiarity. The GDPR and the EU AI Act refer to the principle of subsidiarity as stated in Article 5 of the TEU (The Treaty of European Union, 2012):

> *Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.*

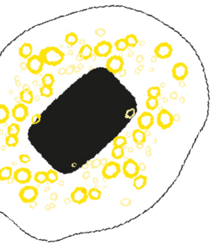
Though this is related to the division of powers instead of technology. Within the DPIA or FRIA, this is better described, asking if the technology is really necessary and if there are less harmful alternatives regarding privacy (Autoriteit Persoonsgegevens, 2024). This is also how organizations should interpret the principle of subsidiarity in the context of technology. Consequently, describing this principle better in the GDPR and EU AI Act would be more comprehensive, as well as including it as a criterion when assessing proportionality.



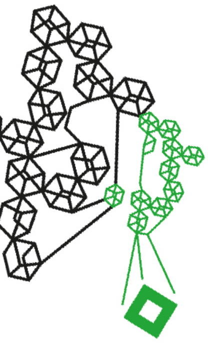
Besides that, human rights organizations/NGO's do express their concerns regarding these regulations, since they remain insufficient in safeguarding the privacy rights of migrants. As seen in the literature, the existing regulations may technically provide protection towards these rights, however, looking in more detail when using technological systems, this remains insufficient. Algorithm Watch (2024b) did research in EU-funded projects that are developing automated (AI) systems used at the European borders. Within these EU projects, the EU has developed a so-called ethics assessment that should ensure privacy rights. However, this assessment appears to be inadequate, as only one project application has ever been prohibited due to ethical complications. All other projects passed the assessment without a thorough review of the potential harms. This is due to the following according to an NGO journalist & researcher: ***"They never challenge the idea or never tackled the question should we be funding this project? They (EU institutions) only say okay we need to fund this, how can we make the project ethical? These organizations say we need this project, make it ethical because it can help achieve the goal, when it is ethical it could have a bigger market and it gets more socially acceptable."***[15] This research contributes to the already existing expectations of these humanitarian organizations by highlighting the created EU "solution", in addition to the DPIA and FRIA, which is again

[15] *Interview code C-35*

showing compliance in a superficial way instead of looking more deeply into the deeper ethical consequences. Moreover, it is evident that these projects are not open for public access, resulting in a lack of transparency and accountability.



One of the Privacy Experts mentioned: ***"We are all at the start of inventing and finding out how to deal with the problem. It would be sufficient to look at the problem together who are already working on it and that you are going to build on it together to do it in a certain way, that would help a lot."*** that collaboration would be key to solving problems like these and to understanding together how to tackle the proportionality problem[16]. This would indeed be sufficient since this creates a broad knowledge hub. However, it is essential to consider and examine the broader implications that arise from this idea. Algorithm Watch discussed these ideas through a panel featuring experts from various fields, including journalism, academia, policy, and civil society institutes. One of the main findings here was that multidisciplinary teams are necessary since the problem of technology use in the migration sector is also influenced by politics and social inequality. Yet, a takeaway from the experiences of such collaborations has been that, in many cases, the primary obstacle to political reform is not a lack of information or data about the dangers of automated border controls. Despite proof of these consequences, policymakers and the general public may continue to favor digital border control technologies and algorithm decision-making at the borders. In such cases, achieving change needs more public involvement to question the beliefs behind technologies used and whether this is fair, especially in the migration context. Unfortunately, for most people, it is hard to be involved in this conversation since migration remains a highly politicized topic, which prevents deeper debates of the underlying issues from happening (Algorithm Watch, 2024a).



To conclude and address the sub-question regarding the expectations relevant public organizations and privacy experts have towards the EU regulatory framework governing proportionality and privacy, a hypothesis has been established before examining the data.

H3: The expectations of relevant public and humanitarian organizations do not align with what is stated in the EU regulatory framework, therefore, these organizations do not know how to effectively safeguard privacy rights.

The results of the analysis partially confirm the hypothesis. The expectations of relevant public organizations do align with the EU regulatory framework, since it is believed that they do

[16] *Interview code B-31*

comply with the regulations when processing data, resulting in non-confirmation of this part. While most organizations believe they do comply with the regulations, it is mostly on a surface level, leaving out the deeper ethical complications related to privacy standards. The part of the hypothesis stating that organizations do not know how to effectively safeguard privacy rights is confirmed because of this. Moreover, the interviews indicated that the principle of proportionality would be stronger in its assessment and implementation when considering the principle of subsidiarity. Unfortunately, this principle is again vaguely and inconsistently included within the EU regulatory framework. Humanitarian organizations have also raised concerns regarding the regulations governing data processing in the migration and border control sector. Research and panels with different experts revealed that there is a lack of transparency, oversight and accountability within assessments and collaborations governing data processing. This part of the hypothesis is thus confirmed, since they do not agree with what is described within the EU regulatory framework, therefore, privacy rights of migrants are not safeguarded effectively.

6.5 Recommendations

This chapter focuses on enhancing the understanding and practical application of the proportionality principle within the EU regulatory framework when an organization or government considers implementing a technological (AI) system in the future. Therefore, this chapter will try to answer the research question: ***What guidelines are necessary to enhance proportionality implementation when using (AI) technologies to protect privacy rights effectively?.*** The answer derives from the findings of the previous research questions and literature. To structure the chapter, it is divided into two components. The first part will focus on the practical guidelines that could be used in the future for assessing proportionality more effectively. The second will focus on overall policy recommendations to embed the principle of proportionality more understandable and effectively within the EU regulatory framework, to enhance the safeguarding of privacy rights.

6.5.1 Practical guidelines

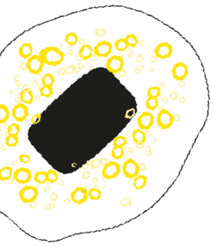
The guidelines are established to translate the abstract principle of proportionality into actionable and practical steps to identify if a technological (AI) system is proportional in its use and could therefore minimize the potential harms to privacy rights. The guidelines are inspired by the established criteria of proportionality in the technological context by the author Karliuk (2022) and the established AI Proportionality Assessment Aid by the Technology Advisory Panel (2025), which developed a framework for the development process for AI systems to assess proportionality. When determining whether data processing complies with legislation, the established criteria by the General Data Protection Regulation EU (2023) for a DPIA focus on three aspects. These three steps include 1) legitimacy, 2) necessity and proportionality, and 3) rights of the data subjects. Under the second step, necessity is assessed through the proportionality (is the intrusion on the rights in balance with the objective) and subsidiary principle (are there less intrusive methods). Although the DPIA framework and the AI Proportionality Assessment Aid do offer guidance and input, they fall short on providing a concrete, comprehensive, and reusable tool for organizations.

Understanding the assessment

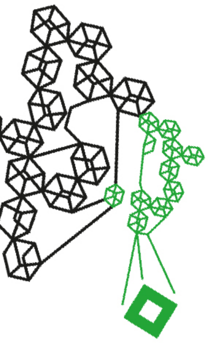
The matrix below can be used to measure all necessary criteria to assess proportionality. The matrix has a score from 1 to 3, meaning that if an organization scores only one time, a score of 1, they should reconsider the technological tool or system. All scores must be at least 2 or 3 to implement the system. When scoring a scale 2, the organization must take additional measures to balance the potential harms. It should be noticed that the assessment of proportionality must be conducted on a case-by-case basis, since different sectors, organizations, objectives, etc., are subject to different regulations. This assessment is intended to serve as a general recommendation. Depending on the context, additional questions may need to be included to make it more comprehensive.

Table 6: Proportionality assessment

Step	Criteria	Questions	Scale (1-3)
Step 1	Legitimacy	- What is the specific objective or public interest the system tries to achieve? - Is this objective legally embedded within the EU regulations? - Is the data processing legally embedded within the EU regulations? - Is the data processing officially documented in a data processing register (Article 30 GDPR)?	1 = Objective is vague and does not align with regulations 2 = Objective clear but does not align with regulations. **OR/AND** Objective clear, stated within regulations but is not documented correctly 3 = The objective is clearly stated, legal, and well-documented under applicable EU or national regulations.



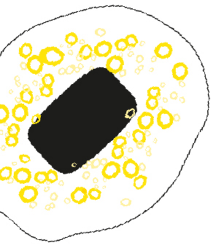
Step 2	Appropriateness	- Does the system actually help to achieve the stated objective? - Is there evidence to support this effectiveness?	1 = No supporting evidence or past examples 2 = Some evidence or examples 3 = Clear empirical evidence
Step 3	Necessity	- Is each data element processed essential for the selected objective? - Is any sensitive data essential for the selected objective?	1 = Data is collected beyond what is required, including unnecessary sensitive data 2 = Most data is justified and some unnecessary sensitive data is included which are not justified 3 = Data only necessary for the objective is collected and sensitive data is justified and minimalized
Step 4	Subsidiarity	- Have less intrusive alternatives been considered to achieve the same objective? - Why are other alternatives not applicable? - How is the selected method the least harmful?	1 = No alternatives are considered or choice is not well-considered 2 = Some alternatives are considered, however, analysis of impact is incomplete or superficial 3 = All alternatives are considered and reasonably excluded
Step 5	Stricto sensu	- Which rights might be infringed when using the selected method? - What are the intended benefits and how might they harm these rights? - How are the benefits justified to harm these rights? - Is there a legal ground for this justification?	1 = Serious rights are infringed without clear justification per right 2 = Some rights are justified, however, lack deeper ethical and legal considerations 3 = A well balanced documentation of the identified risks and justification per right is established
Step 6	Risk acceptance	- Which risks are accepted due to the outweighed benefits? - Have all potential measures to reduce the risks been considered? - Does the data subject that potential (privacy and fundamental) risks exist? - Have all risks related to marginalized data subjects been considered and limited?	1 = Risks are ignored or/and not transparently communicated with data subject 2 = Some risks are considered, not mitigated completely, limited transparency towards data subject 3 = Well identified risks, mitigated and communicated transparently with data subject



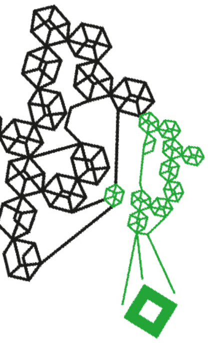
6.5.2 Policy recommendations

Evident from this research is that the principle of proportionality is a broader and complex problem. Therefore, some policy recommendations are established.

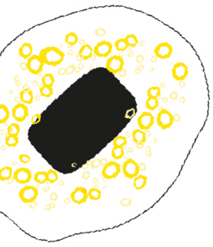
1. The first recommendation relates to the EU regulatory framework governing proportionality. As seen from the literature, the EU AI Act made transparency, control, and oversight requirements exceptions within the migration and border control sector. Including no public registration, project description, assessment such as a FRIA, and above all, compliance with the EU AI Act till 2030. Policy makers should reconsider the EU AI Act and remove the exceptions for the migration and border control sector. The minimum requirement should be to comply with the EU AI Act and to conduct a FRIA. Without these minimum requirements, it is impossible to implement technological (AI) systems that ensure ethical standards. Moreover, evident from the examination of the GDPR and the EU AI Act, the principle of proportionality should be stated more clearly, including, for instance, the criteria within the proportionality assessment. By doing so, organizations could interpret the principle(s) better and hopefully leave less room for their own interpretation and problem amplification to just comply with the regulations.
2. The second recommendation includes appointing more controlling authorities or independent bodies to oversee the execution of DPIAs in organizations and governments. The late execution of these causes unethical implementation of systems due to potentially biased inputs. Ensuring that DPIAs are executed at the actual start of deploying a technological (AI) system causes more ethical considerations, consequently leading to more privacy safeguarding. It is important to note, when more AI systems are being implemented in the upcoming years, oversight and control of FRIAs should be ensured as well.
3. Finally, in order to ensure that proportionality assessments, DPIAs and FRIAs are treated ethically beyond legal compliance, organizations and governments should embed training within their processes. The training should not be limited to Privacy Officers or teams but also include higher-level decision-makers within these organizations. These decision-makers often carry the responsibility to revise the advice of the Privacy Officers and make a final decision on considered technological systems, even when certain risks may need to be accepted to reach the objective. If multiple layers in the organization do understand all steps within the proportionality assessment, a well-considered ethical considered decision could be made.



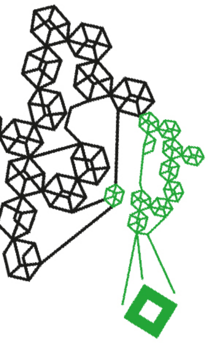
To conclude, the proposed practical guidelines (proportionality assessment) and policy recommendations aim to operationalize the principle of proportionality more effectively by understanding, assessing, and implementing the principles consistently across organizations. By doing so, the privacy rights of migrants are safeguarded more effectively, since ethical implications are considered more deeply.



7. Conclusion and discussion



The research investigated the EU regulatory framework governing technological (AI) systems within the migration and border sector, especially focusing on the inclusion of the principle of proportionality. The examination of these elements were important to understand the extent of the safeguarding of the privacy rights of migrants. Therefore, the research seeks to answer the main research question: ***To what extent and how is proportionality embedded in the EU regulatory framework and how can it be enhanced to better align with public organizations' expectations and privacy protection when using (AI) technologies in border management?*** Through the qualitative analysis, the inclusion of proportionality within the EU regulatory framework, the gaps regarding this inclusion compared to practical implementation, and relevant expectations were examined. The findings demonstrate that while the principle of proportionality is formally included within the EU regulations governing technologies and AI systems, it remains an abstract, normative, and broad interpretable principle. Therefore, the extent to which the principle of proportionality and other safeguard mechanisms are applied in practice remains insufficient, especially in the migration and border control sector. The legal analysis and interviews confirm that while the current EU regulatory framework serves as a foundation for legal compliance, it lacks clarity and enforceability to be consistent and effective in safeguarding against ethical complications that may arise. This is evident through the checkbox approach, where proportionality is applied superficially, lacking any deeper ethical considerations in order to comply with the law. In practice, these organizations refer back to DPIAs as the primary source assessing privacy, though these are often executed too late, leading to biased inputs, resulting in accepting privacy risks faster than they should. In addition, multiple exceptions from risk assessments and publicly available data regarding the systems create a lack of oversight, accountability, and transparency. Therefore, expectations from privacy experts and public governmental organizations regarding the principle of proportionality and overall safeguarding of privacy rights were examined to find a solution concerning enhancing privacy protection when using (AI) technologies. As a result of better aligning the EU regulatory framework with expectations to safeguard privacy rights when deploying technological (AI) systems in the future, some recommendations have been established.

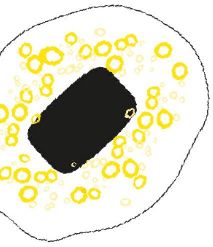


Firstly, a proportionality assessment is created based on six criteria, including legitimacy, appropriateness, necessity, subsidiarity, stricto sensu, and risk acceptance. To effectively integrate these criteria in the migration and border control sector, some additional policy recommendations are proposed. These include reconsidering the EU AI Act's exceptions in the migration and border control sector, integrating the proportionality assessment criteria within relevant regulations to enhance understanding and practical execution, appointing more controlling bodies to check on DPIAs and FRIAs, and enhancing training within organizations at multiple decision-making levels to safeguard privacy rights more effectively.

7.1 Contributions and implications

The research contributes to multiple scientific and societal debates on AI and technological governance, data and fundamental rights protection, through the examination of the proportionality principle within the EU migration and border management sector. It addresses a significant research gap recognized in the literature: while the idea of proportionality is legally stated in both the GDPR and the EU AI Act, there continues to be a lack of clarity and academic consensus on how it should be implemented in practice (Kloza & Drechsler, 2024). Scholars such as Karliuk (2022) and McGregor & Molnar (2023) have highlighted the vagueness of proportionality as a legal criterion, as well as the problems of ensuring consistent implementation among MS. The study also corresponds with requests from Warthon (2024) and Alarcón et al. (2024) for the establishment of more practical proportionality frameworks in highly sensitive fields such as migration and border control. Through the examination and creation of a concrete proportionality assessment and policy recommendations, this research addresses the gap between a policy problem and its practical execution. The research has also contributed to the societal relevance, particularly around the rise of reliance on technological (AI) systems within the migration sector. Human rights organizations such as Amnesty International (2024) and Statewatch (2023) have expressed their worries about the human rights/privacy breaches these technologies may have on migrants. These concerns are supported by this research, indicating how ambiguous legislative criteria and late executions of DPIAs allow privacy risks to be overlooked or accepted without proper examination. Moreover, the research has contributed to the findings of Molnar (2023), recommending further investigation on how the EU should create a human-rights-based approach to the development and deployment of technologies used at the borders. The study offers practical tools and policy recommendations to promote the effective protection of the privacy rights of migrants.

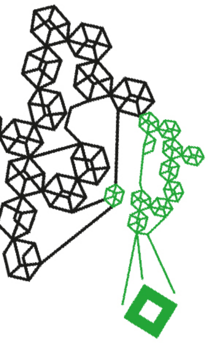
As seen above, the research offers relevant insights for academic and policy domains involved in technological developments within the migration and border control sector. While this study does not try to claim that policy can be changed overnight, the results present meaningful contributions on how to better include and execute proportionality. The assessment will provide public organizations with a hands-on tool, which can also be used in other sectors than migration. Moreover, the study will draw more attention to the ethical concerns and practical gaps missing to ensure the privacy rights of migrants. Although the principle of proportionality remains somewhat vague and broad, the study tried to make the principle a bit more understandable and useful. Future developments will reveal whether this is the case and how the EU institutions will apply the proportionality assessment and policy recommendations to their policies.



7.2 Limitations of the research

While this study presents a thorough examination of how the principle of proportionality could be better included and examined in practice when using technological (AI) systems, a few limitations exist that should be addressed.

The first limitation concerns the number and composition of interview respondents. While the study focused on the EU regulatory framework, interviews with governmental organizations were restricted to representatives of governmental institutions within the Netherlands. This was due to several circumstances, including time constraints, the difficulty of obtaining access to EU-level organizations, and the sensitive/politicized nature of the topic, which made respondents hesitant to participate. Nonetheless, the respondents who conducted an interview are high-level representatives in the migration sector, which still helped with creating depth and reliability in the research. Furthermore, the number of respondents for the human rights organizations is limited, as many lacked the specific knowledge regarding proportionality or data processing policies within the migration context. Therefore, the study strengthened its findings with literature and conducted earlier research. The second limitation concerns the focus on AI systems within this research. As earlier stated within the results, it was evident during the research that AI systems are not yet fully operational within the migration sector. While the initial focus was to examine AI systems, the study shifted towards technological and automated systems with a human decision-making aspect, as these are currently in use. Consequently, some of the findings are anticipatory, and circumstances could be changed within this year, for instance, the exception of AI systems in the migration sector to be compliant with the EU AI Act in 2030. Nonetheless, the ethical questions surrounding proportionality remain relevant and are even more important for the future when AI systems become fully operational. Lastly, the research focused mainly on fundamental rights and migrants, in contrast to perspectives that position innovation and efficiency above these aspects. Therefore, the study may have a more human rights and policy approach rather than an approach for technical opportunities.



7.3 Recommendations for future research

This thesis focused mainly on the examination of the proportionality principle. As seen in the results, it would be relevant to also examine the principle of subsidiarity to make the safeguarding of privacy rights more comprehensive. An example could be to establish a similar assessment to assess and understand the principle of subsidiarity more effectively. Moreover, it would be sufficient to investigate within the EU institutions how they perceive the principle of proportionality problem and how they understand and examine the principle in practice. An additional feature could be to compare the EU institutions with the United States institutions, since data protection and processing are handled differently. The US is more market and technological driven, therefore, it could give valuable insights in how the US is incorporating, assessing proportionality and safeguarding migrants' privacy rights.

Additionally, the study mainly methods existed from qualitative desk research, it would be interesting to examine if quantitative methods would give a different outcome. Since AI systems are not used completely at the moment of the research, it would also be sufficient to conduct the same research again when AI technologies are fully operational within the migration sector. Also, within 5 years, when these AI systems within the migration sector need to be compliant with the EU AI Act, it would be interesting to see if anything will change regarding ethical complications. Lastly, a follow-up from this research would be valuable to assess whether the recommended guidelines and policy changes are effective in enhancing the safeguard of privacy rights.

Bibliography

Abbas, S. (2024). *Different Types of Sampling Techniques in Qualitative Research*. Sago. https://sago.com/en/resources/blog/different-types-of-sampling-techniques-in-qualitative-research/

AI Act (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

Ajoodha, T., & Browne, J. (2025). *Fundamental Rights Impact Assessments: What are they? How do they work*? In Micro-Insights Series. https://cedpo.eu/wp-content/uploads/CEDPO-micro-insight-paper-fundamental-rights-impact-assessments.pdf

Alarcón, Á., Gigena, F. G., & Coppi, G. (2024). *“Smart borders “and the making of a humanitarian crisis*. Access Now. https://www.accessnow.org/smart-borders-and-the-making-of-a-humanitarian-crisis/

Algorithm Watch. (2024a). How to Rethink Tech in Migration - AlgorithmWatch. AlgorithmWatch. https://algorithmwatch.org/en/how-to-rethink-tech-in-migration/Algorithm Watch. (2024). *No Access to Border Tech: More Transparency in EU Research on Border Surveillance Technology needed - AlgorithmWatch*. AlgorithmWatch. https://algorithmwatch.org/en/automation-on-the-move-policy-brief/

Amnesty International. (2024b). *Defending the rights of refugees and migrants in the digital age.* In Amnesty.org (Vol. 4, Nummer 1). https://doi.org/10.1177/2056305118764432

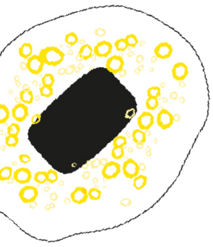
Amnesty International. (2024). *THE DIGITAL BORDER: MIGRATION, TECHNOLOGY, AND INEQUALITY*. https://www.amnestyusa.org/wp-content/uploads/2024/05/The-Digital-Border-Migration-Technology-and-Inequality-1.pdf

Andreou, A. S. (2023*). E-Securing the EU Borders: AI in European Integrated Border Management.* Journal of Politics and Ethics in New Technologies and AI, 2(1). https://doi.org/10.12681/jpentai.34287\

Autoriteit Persoonsgegevens. (2024). *Basisprincipes voor het gebruik van drones met camera.* https://www.autoriteitpersoonsgegevens.nl/themas/cameratoezicht/drones/basisprincipes-voor-het-gebruik-van-drones-met-camera

Autoriteit Persoonsgegevens. (2025). *EU AI Act.* https://www.autoriteitpersoonsgegevens.nl/en/themes/algorithms-ai/eu-ai-act

Belderbos, H. (2025). *AI for border control speed and security*. Open Access Government. https://www.openaccessgovernment.org/ai-for-broader-control-speed-and-security/187217/



Better Care Network. (2023). *Implementation Mechanisms*. https://bettercarenetwork.org/practitioner-library/implementation-mechanisms

Bouvier, C. (2024). *A dangerous precedent: how the EU AI Act fails migrants and people on the move.* PICUM. https://picum.org/blog/a-dangerous-precedent-how-the-eu-ai-act-fails-migrants-and-people-on-the-move/

Charter of Fundamental Rights of the European Union. (2000). https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Citizen Information. (2023). *The Schengen area*. https://www.citizensinformation.ie/en/government-in-ireland/european-government/european-union/schengen-area/

Collins. (2024). *Support a policy*. https://www.collinsdictionary.com/dictionary/english/support-a-policy

CyberLaws Europe. (2023). *What does "Human-Centric AI" mean? – Legal definition*. CyberLaws. https://www.cyberlaws.it/en/2023/what-does-human-centric-ai-mean-legal-definition/

DataGuard. (2024). *What is a regulatory framework?* https://www.dataguard.co.uk/blog/what-is-a-regulatory-framework/#:~:text=A%20regulatory%20framework%20is%20a%20set%20of%20rules%2C%20regulations%2C%20and,government%20or%20other%20regulatory%20bodies.

Delinavelli, G. (2023). *Wat is het verschil tussen een DPIA en een FRIA?* PONT Data&Privacy. https://privacy-web.nl/nieuws/wat-is-het-verschil-tussen-een-dpia-en-een-fria/

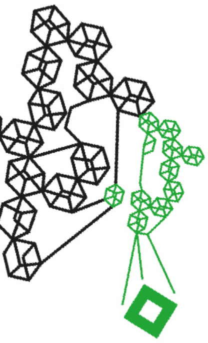
Dijstelbloem, H., & Broeders, D. (2014). *Border surveillance, mobility management, and the shaping of non-publics in Europe*. European Journal of Social Theory, 18(1), 21–38. https://doi.org/10.1177/1368431014534353

EU Artificial Intelligence Act. (2025). *EU Artificial Intelligence Act*. https://artificialintelligenceact.eu/article/3/

European Commission. (2011). *Smart borders - options and the way ahead*. In LexUriServ.do (COM (2011) 680 final). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0680:FIN:EN:PDF

European Commission. (2024). *Shaping Europe's Digital Future*. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Commission. (2024). *Smart Borders package*. Migration And Home Affairs. https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-



asylum-and-migration-glossary/glossary/smart-borders-package_en#:~:text=Set%20of%20measures%20consisting%20of,non%2DEU%20travellers%2C%20while%20at

European Council. (2024). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

European Data Protection Supervisor. (2019). *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*. https://www.edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf#:~:text=The%20necessity%20and%20proportionality%20of%20a%20legislative%20measure,that%20involves%20processing%20of%20personal%20data%20must%20comply.

European Data Protection Supervisor. (2024). *Necessity & proportionality. European Union.* https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

European Data Protection Supervisor. (2018). *The History of the General Data Protection Regulation.* https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=The%20GDPR%20is%20now%20recognised%20as%20law%20across,data%20protection%20reform%20process%20from%201995%20to%202018.

European Parliament. (n.d*.). Fundamental rights in the EU. Fundamental Rights in The EU.* https://www.europarl.europa.eu/about-parliament/en/democracy-and-human-rights/fundamental-rights-in-the-eu

European Parliament. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530

European Parliament. (2021). Artificial intelligence at EU borders. In *Members' Research Service* (Report PE 690.706; p. I–II). https://doi.org/10.2861/91831

European Parliament. (2023). *EU AI Act: first regulation on artificial intelligence.* https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

European Union Agency for Fundamental Rights. (2020). *What are fundamental rights?* European Union Agency For Fundamental Rights. https://fra.europa.eu/en/content/what-are-fundamental-rights

Forti. (2021). *AI-Driven Migration Management Procedures: fundamental rights issues and regulatory answers* (BioLaw Journal, 2 (2021), 433-451). https://ssrn.com/abstract=3877083

Frontex. (n.d.). *Operations*. https://www.frontex.europa.eu/what-we-do/operations/operations/#:~:text=Frontex%2C%20the%20European%20Border%20and,and%20tackling%20cross%2Dborder%20crime.

Galdon Clavell, G. (2017). *Human rights are at stake when we cross a border*. Dataethics.eu. https://dataethics.eu/protect-rights-automated-borders/

Gandhi, S. (2024). Frontex as a hub for surveillance and data sharing: Challenges for data protection and privacy rights. *Computer Law & Security Review*, *53*, 105963. https://doi.org/10.1016/j.clsr.2024.105963

GDPR (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

General Data Protection Regulation EU. (2023). Data Protection Impact Assessment (DPIA). GDPR.eu. https://gdpr.eu/data-protection-impact-assessment-template/

Gonzalez Riedel, D., & Idema, S. (2024*). Understanding the intersection between the EU's AI Act and privacy compliance.* Compact. https://www.compact.nl/articles/understanding-intersection-between-eus-ai-act-and-privacy-compliance/

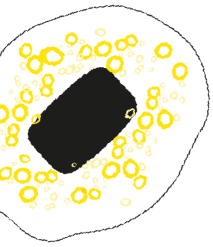
Government mandate (2024). https://dictionary.cambridge.org/example/english/government-mandate

Hadley, T. (2022). *Understanding purposes of regulation: a case example in mental health.* PubMed.https://pubmed.ncbi.nlm.nih.gov/10309380/#:~:text=The%20primary%20regulatory%20purpose%20is,development%2C%20(3)%20protectionism.

Haefner, N., Parida, V., Gassmann, O., & Wincent, J. (2023). *Implementing and scaling artificial intelligence: A review, framework, and research agenda*. Technological Forecasting And Social Change, 197, 122878. https://doi.org/10.1016/j.techfore.2023.122878

Hendow, M., Cibea, A., & Kraler, A. (2015). *Using technology to draw borders: Fundamental rights for the Smart Borders Initiative*. Journal of Information, Communication and Ethics in Society, 13(1), 39–57. https://doi.org/10.1108/jices-02-2014-0008

Hirvonen. (2023). *Smart Borders Package improves EU border management*. Ministry of the Interior. https://intermin.fi/en/border-management/smart-borders#:~:text=In%20spring%202013%2C%20the%20Commission,come%20operational%20in%20November%202023



IBM. (2020). *What is linear regression?* https://www.ibm.com/topics/linear-regression#:~:text=Linear%20regression%20analysis%20is%20used,is%20called%20the%20independent%20variable.

Jeandesboz, J. (2016). *Smartening border security in the European Union: An associational inquiry*. Security Dialogue, 47(4), 292–309. https://doi.org/10.1177/0967010616650226

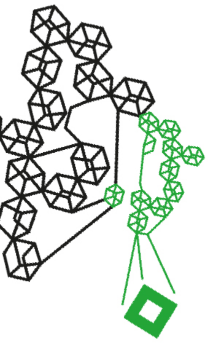
Karliuk, M. (2022). *Proportionality principle for the ethics of artificial intelligence*. AI And Ethics. 3(3), 985–990. https://doi.org/10.1007/s43681-022-00220-1

Kieran, B., Cascales, F.A., Thomi, L., & Veit, M. (2019) *Are smart walls smart solutions?* The impact of technologically charged borders on human rights in Europe. *Global Campus Human Rights Journal*, (3) 173-209 http://dx.doi.org/10.25330/483

Kourinian, A., & Brown, M. (2024). *Addressing Transparency & Explainability When Using AI Under Global Standards*. In *Bloomberg*. https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2024/01/addressing-transparency-and-explainability-when-using-ai-under-global-standards.pdf%3Frev=-1#:~:text=Transparency%20answers%20the%20question%20%E2%80%9Cwhat,Framework%20(AI%20RMF%201.0).

Kumar, P. (2023). *Privacy: A Fundamental Human Right Explored*. The Law Institute. https://thelaw.institute/privacy-and-data-protection/privacy-fundamental-human-right/

Lehtonen, P., & Aalto, P. (2017). *Smart and secure borders through automated border control systems in the EU. The views of political stakeholders in the member states.* European Security, *26*(2), 207–225. https://doi.org/10.1080/09662839.2016.1276057

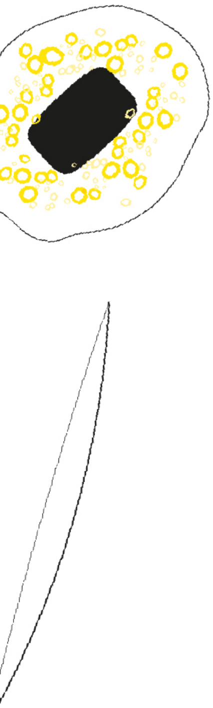


Luo, A. (2023). *Content Analysis | Guide, Methods & Examples*. Scribbr. https://www.scribbr.com/methodology/content-analysis/

Madiega, T. (2024). *Artificial intelligence act. In EU Legislation in Progress.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf#:~:text=The%20AI%20act%2C%20the%20first%20binding%20worldwide%20horizontal,Some%20AI%20systems%20presenting%20%27unacceptable%27%20risks%20are%20prohibited.

Mahendra, S. (2024). *How AI learns: datasets and data processing*. Artificial Intelligence +. https://www.aiplusinfo.com/blog/how-ai-learns-datasets-and-data-processing/

Mahmutovic, A., & Olson. (2020). *European Union smart borders: An examination of its structural impacts on human rights versus national sovereignty needs*. Hamdard Islamicus, *43(2),* 774–784



McCormick, P. K., Bitson, W., & Mohamad, Z. (2025). EU Borderveillance: Maritime Surveillance and Third Country Agreements. In Heinrich Böll Stiftung – Middle East Office, EU Borderveillance [Report]. https://refugees-partners.org/wp-content/uploads/2025/01/EUBorder.pdf

McCombes. (2023). *Literature review*. Scribbr. https://www.scribbr.com/methodology/literature-review/

McGregor, L., & Molnar, P. (2023). *Digital Border Governance: a human rights-based approach.* In Digital Border Governance: A Human Rights Based Approach. https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf

Medelyan, A., PhD. (2024). *Coding Qualitative Data: How to Guide*. Thematic. https://getthematic.com/insights/coding-qualitative-data/

Middleton, F. (2023). *Reliability vs. Validity in Research | Difference, Types and Examples*. Scirbbr. https://www.scribbr.com/methodology/reliability-vs-validity/

Migration Data Portal. (2022). *Migration and data protection.* https://www.migrationdataportal.org/themes/migration-and-data-protection

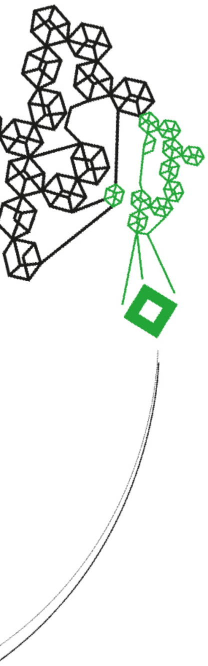
Migration and Home Affairs (n.d.). *European Integrated Border Management*. https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/european-integrated-border-management_en#:~:text=The%20European%20integrated%20border%20management,as%20migrant%20smuggling%2C%20trafficking%20in

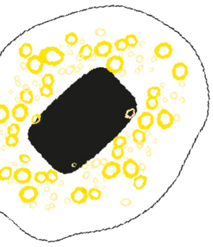
Ministry of the Interior and Kingdom Relations (2022). *Impact Assessment Fundamental Rights and Algorithms.* fundamental-rights-and-algorithms-impact-assessment-fraia (5).pdf

Molnar, P. (2020). *Technological Testing Grounds | Migration Management Experiments and Reflections from the Ground Up.* EDRi. https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf

Molnar, P. (2023). *EU's AI Act Falls Short on Protecting Rights at Borders*. Just Security. https://www.justsecurity.org/90763/eus-ai-act-falls-short-on-protecting-rights-at-borders/

Nikolopoulou, N. (2022). *What Is Content Validity? | Definition & Examples*. Scribbr. https://www.scribbr.com/methodology/content-validity/#:~:text=Content%20validity%20evaluates%20how%20well,four%20types%20of%20measurement%20validity.





NOREA DPIA. (2020). *Handreiking Data Protection Impact Assessment.* https://www.norea.nl/uploads/bfile/2a7746e6-f5ee-4426-b12c-ba9217608275

OECD. (2024). *AI Policy Observatory Portal*. https://oecd.ai/en/dashboards/ai-principles/P9

OECD. (2015). *Regulatory Policy Outlook 2015*. OECD. https://www.oecd.org/en/publications/oecd-regulatory-policy-outlook-2015_9789264238770-en.html

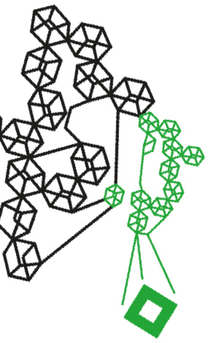
Organization of Economic Cooperation and Developments. (2013). *OECD legal instruments*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Orav, A., & D'Alfonso, A. (2016). *Smart Borders: EU Entry/ Exit System*. In EPRS | European Parliamentary Research Service (PE 586.614). https://brexitlegal.ie/wp-content/uploads/2019/08/Smart-Borders-People.pdf

Pass, J. (2024). *Objective vs. Subjective Perspectives: Understanding the Difference and Why It Matters* — Simply Put Psych. Simply Put Psych. https://simplyputpsych.co.uk/psych-101-1/objective-vs-subjective-perspectives

Peerboom, F. (2022). *Protecting Borders or Individual Rights? A Comparative Due Process Rights Analysis of EU and Member State Responses to "Weaponised" Migration.* European Papers. https://doi.org/10.15166/2499-8249/580

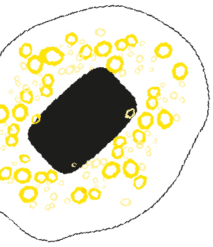
Pina, M. C. (2025). *AI in the context of border management, migration and asylum in the EU: technological innovation vs. fundamental rights of migrants in the AI Act*. Official Blog Of UNIO. https://officialblogofunio.com/2025/02/15/ai-in-the-context-of-border-management-migration-and-asylum-in-the-eu-technological-innovation-vs-fundamental-rights-of-migrants-in-the-ai-act/



Rehman, T. (2022). *Fundamental Rights vs. Human Rights — What's the Difference?* https://www.askdifference.com/fundamental-rights-vs-human-rights/

Rintamäki, T., & Pandit, H. J. (2024). *Towards an automated AI Act FRIA tool that can reuse GDPR's DPI. In Adapt Centre.* https://files.osf.io/v1/resources/538wy/providers/osfstorage/676352b68dce3a7450a335f5?format=pdf&action=download&direct&version=1

Rintamäki, T., Golpayegani, D., Lewis, D., & Pandit, H. J. (2023). *High-Risk Categorisations in GDPR vs AI Act: Overlaps and Implications.* file:///C:/Users/DK851AK/Downloads/IEEE_ACCESS_High_Risk_Categorisations_in_GDPR_vs_AI_Act_Overlaps_and_Implications%20(1).pdf



Shabani, M., & Borry, P. (2017). *Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation*. European Journal Of Human Genetics, 26(2), 149–156. https://doi.org/10.1038/s41431-017-0045-7

Spinhoven, F. (2025). *EU AI Act: clarification or confusion over the AI definition*. https://www.conclusion.nl/en/ai-360/news/eu-ai-act-clarification-or-confusion-over-ai-definition

Statewatch. (2023). *Europe's Techno Borders*. In EuroMed Rights. https://euromedrights.org/wp-content/uploads/2023/07/EuroMed-Rights_Statewatch_Europe-techno-borders_EN-1.pdf

Technology Advisory Panel. (2025). *AI Proportionality Assessment Aid*. https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/AI-Assessment-Framework.pdf

Temirov, S. (2025). *Data Protection and Privacy Challenges of Refugees in the Digital Age*. International Women's Network in Estonia. https://iwne.ee/data-protection-and-privacy-challenges-of-the-refugees-in-the-digital-age-a-critique-of-consent-under-coercion-data-sharing-and-access/

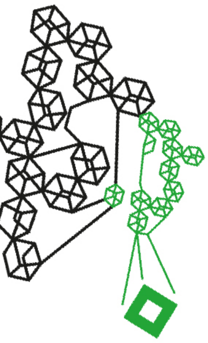
The Treaty on European Union (2012). https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

Thibodeaux, W. (2016*). What Is an Open-Ended Interview?* Chron - Small Business. https://smallbusiness.chron.com/openended-interview-23923.html

Thiel, J. (2022). Whitepaper - Checkbox Compliance - Yields. Yields.io. https://www.yields.io/blog/whitepaper-checkbox-compliance/

Van Rijmenam, M. (2023). *Privacy in the Age of AI: Risks, Challenges and Solutions*. CSP | Strategic Futurist Speaker. https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/#:~:text=In%20the%20context%20of%20AI,based%20on%20their%20personal%20data.

Vavoula, N. (2021). *Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism*. European Journal Of Migration And Law, *23*(4), 457–484. https://doi.org/10.1163/15718166-12340114



Warthon, M. (2024). *Restricting access to AI decision-making in the public interest: The justificatory role of proportionality and its balancing factors.* Internet Policy Review. https://policyreview.info/articles/analysis/restricting-access-to-ai-decision-making

What is the EU regulatory framework? (2024). https://www.6clicks.com/resources/answers/what-is-the-eu-regulatory-framework

Zaidan, E., & Ibrahim, I. A. (2024). *AI governance in a complex and rapidly changing regulatory landscape: A Global perspective*. Humanities and Social Sciences Communications, 11(1). https://doi.org/10.1057/s41599-024-03560-x

Appendix

Appendix 1: Coding scheme sub-question 3

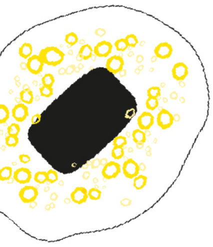
A = governmental public organizations
B = privacy experts
C = civil society

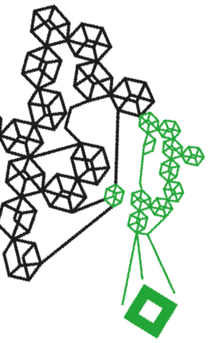
Type	Number	Open code	Sub code	Main code
A	01	Often is seen in practice that the DPIA is executed halfway in the process of system implementation.	To late execution of DPIA	Insufficient integration of privacy during system implementation
A	02	The DPIA is actually done a lot at the end of the process.	To late execution of DPIA	
B	03	The theory is, of course, someone wants to develop a system, the organization has to go through a compliance route and should do a DPIA in advance. Practice shows that this does not always happen.	To late execution of DPIA	
B	04	Organizations should conduct a DPIA in advance; otherwise, they risk investing excessively in the development process without fully understanding the privacy implications. If the DPIA is completed too late, it is frequently filled in with the bias of 'it's good this way,' which nearly assures organizational resistance and potential failure.	To late execution of DPIA leading to biased implementation	
A	05	The execution of DPIA's is still very much at the beginning what is surprising.	Did not executed a lot of DPIA's yet	

A	06	Sometimes the organization finds out that a certain system exists and that certain personal data is processed. The organizations thinks they don't have to carry out a DPIA, therefore doing it afterwards.	Too late execution of DPIA	
A	07	The system has already been implemented and the only thing you can do about that, is discussing the risks that derive from the system and have to indicate how the organization will deal with those risks.	Accepting risks due to late DPIA execution	
B	08	Sometimes the organization discovers things being done in practice while if they had done the DPIA in advance, they would never have started the process of the system.	Accepting risks due to late DPIA execution	
A	09	Within the DPIA you do describe what risks you are going to accept as an organization.	Accepting risks	
A	10	In the DPIA you are not writing down that something isn't proportional, however the organization describes that the policymakers have failed to provide a specific basis for these risks and do accept them.	Accepting risks based on incompetent regulation	Reliance on regulations despite ambiguity
A	11	Using automated systems based on references list described within the law.	Using automated systems based on regulations	

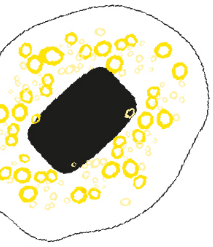
A	12	Asking for personal data is legally identifiable.	Regulatory basis	
A	13	But the processing of personal data, necessary and proportionate, also falls under this, which is often described and interwoven in the law and that is the basis of processing.	Regulatory basis	
A	14	Will not achieve the goal if there is no personal data processing. Looking at proportionality, think about it so carefully that processing in such a way that you don't have to take extra information or steps if it is not necessary.	Proportionate processing of data	Lack of clarity in the principle of proportionality
B	15	Ultimately, the purpose is to determine whether the chosen systems are consistent with the stated objectives. The guiding idea is to avoid utilizing technologies or processes that do not serve a clear purpose, though in practice, there may be exceptions.	Inadequate proportionality execution	
A	16	Sometimes the problem for which the technology should be used is too little to be appropriate. Therefore, the organizations tries to frame the problem bigger in order to justify the technology.	Framing the principle of proportionality	
A	17	In the final stage, a decision is taken on whether the organization chooses to proceed with	Principle of proportionality unclear resulting in no further deployment system	

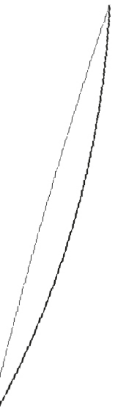
		the system. In this example, implementation has not yet occurred since the problem of proportionality is still being discussed internally until there is a clear solution to resolve it.		
B	18	Proportionality is always a part that is described within the DPIA together, since noticing that it is still difficult for the organization to make that decision. What does it actually mean?	Principle of proportionality unclear	
A	19	Still unclear how to assess a proportionality since people don't understand what is meant by the concept.	Principle of proportionality unclear	
A	20	Trying to create a privacy group to execute and implement privacy when processing data	Privacy group	Utilize privacy teams
A	21	Looking at the risk through multidisciplinary team, focusing on privacy risks and how to mitigate them.	Privacy team	
B	22	Work with "privacy by design" and create organizational awareness and a team responsible for privacy.	Privacy team	
B	23	Created a privacy office which looks very closely at what data is processed and if it concerns special personal data. If that is the case, they will focus on privacy. The checks and measures are very	Privacy and AI office	



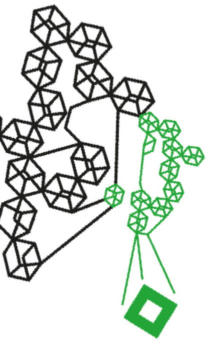


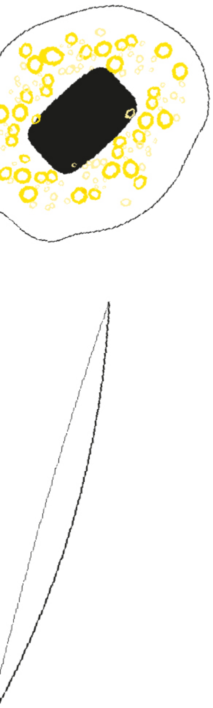
		much in place there. The privacy office is therefore presented in the AI review committee which looks at AI implementations.		
A	24	There is very little AI or high risk in the sense that we see AI in the world as advanced tooling that contains training data or is tested with. There is virtually no such thing within our organization. According to the AI Act and the definition as it is described in it, there is simply very little.	No AI as defined in EU AI Act	No AI implementation (yet)
A	25	Looking at the definition of AI as it is stated in the AI Act, the organization isn't using these systems at the moment.	No AI as defined in EU AI Act	
B	26	Only use automated systems to enhance the speed of processes.	Automated systems	
A	27	Implementing the EES system later this year.	AI system not implemented yet	
A	28	Automated systems to make decisions, however still using humans at the end of the decision line.	Automated systems with final human decision making	Final human decision making
A	29	Using a spider web mechanism to make a risk categorization of data processing. Then identify which risks will be accepted and how to mitigate where possible.	Risk matrix	Possible solutions
A	30	Always integrate necessity and subsidiarity when assessing proportionality.	Principles	



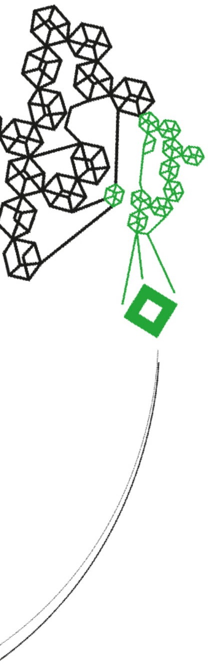


B	31	We are all at the start of inventing and finding out how to deal with the problem. It would be sufficient to look at the problem together who are already working on it and that you are going to build on it together to do it in a certain way, that would help a lot.	Collaboration	
C	32	When something happens regarding human rights breaches, they always fall back on the unawareness of the technology being used.	Relying on technological unawareness	Unawareness
C	33	We can give critique but the organizations do not have the expertise to give fully understanding of what is happening.	Lack of expertise and awareness	
C	34	You see that other sectors such as education do have to comply but not in migration. There is a specific reason why because these governments spent millions of euros to develop emotion recognition technologies over the years within border control and do not want to waste it.	Non-compliance EU AI Act	Non-compliance
C	35	However, then you actually read it in some of the documents and they never challenge the idea or never tackled the question should we be funding this project? They only say okay we need to fund this, how	Ethical assessment non-compliance	



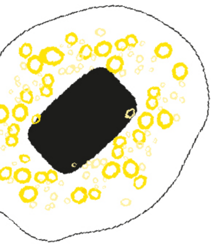


		can we make it ethical? These organizations say we need this project, make it ethical because it can help achieve the goal, when it is ethical it could have a bigger market and it gets more socially acceptable.		

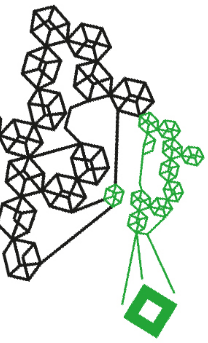


Appendix 2: Proportionality criteria derived from the GDPR (2016)

Criteria	Article	Definition or comment
Stricto sensu Stricto sensu refers to the broader definition of proportionality, meaning that the technology used should not impose unnecessary constraints on individuals or rights (Karliuk, 2022; Amnesty International, 2024).	Legal provision 170	*"In accordance with the* ***principle of proportionality,*** *as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective."* This principle derives from the TEU and the CFR.
	Article 5.1 (a-f)	Additionally, the GDPR describes other standards regarding the processing and storing of personal data, covered within Article 5.1 (sub-a-f). Here, the regulation refers to standards such as lawfulness, fairness, transparency, data minimization, accuracy, confidentiality, accountability, and integrity.
	Article 23 (b-c)	Refers to exceptions of restricting the fundamental rights of individuals when public and national security is the goal of the technology, as with the use of AI at borders to enhance security of its MS: *"Union or Member State law to which the* ***data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided*** *for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and* ***is a necessary and proportionate measure in a democratic society to safeguard****"*
	Legal provision 73	*"Restrictions concerning specific principles ..... may be imposed by Union or Member State law, as far as necessary and* ***proportionate*** *in a democratic society to safeguard public security, including the protection of human life ....., including the safeguarding against and the prevention of threats to public security…"*
	Legal provision 129	*"The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate,*



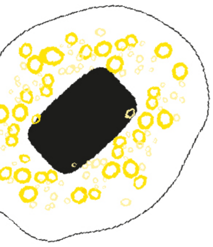
		*necessary and **proportionate** in view of ensuring compliance with this Regulation.. "*
	Legal provision 47	*"The **legitimate** interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the **fundamental rights and freedoms of the data subject are not overriding**, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller."*
Legitimacy Legitimacy refers to the fact that the used technology should be in line and prescribed within the law (Karliuk, 2022; Amnesty International, 2024)	Article 6.1 (a-f)	*"Processing shall be lawful only if and to the extent that at least one of the following applies:…"*
	Article 5 (b)	*"Personal data shall be collected for specified, explicit and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for **archiving purposes in the public interest** …. shall in accordance with Article 89(1), **not be considered to be incompatible with the initial purposes** ('purpose limitation')"*
	Article 14.5 (b)	*"In such cases the controller shall take **appropriate** measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available"*
	Legal provision 39	*"Any processing of personal data should be **lawful** and fair… the specific purposes for which personal data are processed should be explicit and **legitimate** and determined at the time of the collection of the personal data."*
	Legal provision 40	*"In order for **processing to be lawful,** personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.."*

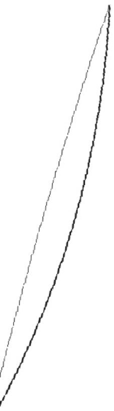


	Article 5.1 (c)	*" Personal data should be; adequate, relevant, and limited to what is* ***necessary*** *in relation to the purposes for which they are processed"*
Necessity The used technology should be strictly necessary to achieve the goal (Karliuk, 2022; Amnesty International, 2024)	Article 6.1 (f)	*(f) processing is* ***necessary*** *for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.* ***Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."***
	Article 6.4	*"Where the processing for a purpose other than that for which the* ***personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate*** *measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected…"*
	Legal provision 39	The same as stated in Article 5.1 (c): *"The personal data should be adequate, relevant and limited to what is* ***necessary*** *for the purposes for which they are processed."*
	Legal provision 50	*"The processing of personal data for purposes other than those for which the personal data were initially collected should be* ***allowed only where the processing is compatible with the purposes for which the personal data were initially collected."***
Appropriateness The used technology	Legal provision 71	*"In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal*

should be appropriate when achieving the goal (Karliuk, 2022; Amnesty International, 2024)		*data are processed,* ***the controller should use appropriate mathematical or statistical procedures*** *for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and he risk of errors is minimised …* *… Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions."*
	Legal provision 74	*In particular, the controller should be obliged to implement* ***appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation****, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.*
	Legal provision 78	*"The protection of the rights and freedoms of natural persons with regard to the* ***processing of personal data require that appropriate technical and organisational measures*** *be taken to ensure that the requirements of this Regulation are met….. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders."*
	Legal provision 102	*"Member States may conclude international agreements which involve* ***the transfer of personal data*** *to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include* ***an appropriate level of protection for the fundamental rights of the data subjects."***
	Legal provision 156/ Article 24	*"The* ***processing of personal data for archiving purposes in the public interest…should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.*** *Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation."*

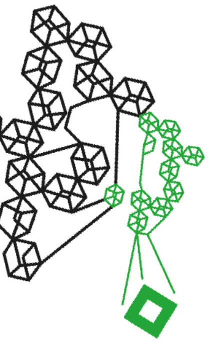
	Article 5.1 (b) Applies also to necessity and legitimacy	*"Personal data shall be;* ***collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes****; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')"*
	Article 9.1 Article 9.1 (b)	*"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs … of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."* Unless: *"Processing is* ***necessary for the purposes*** *of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law….* ***appropriate*** *safeguards for the fundamental rights."* Applies also to the necessity criteria





Appendix 3: Proportionality criteria derived from the EU AI Act (2024)

Criteria	Article	Definition or comment
Stricto sensu Stricto sensu refers to the broader definition of proportionality, meaning that the technology used should not impose unnecessary constraints on individuals or rights (Karliuk, 2022; Amnesty International, 2024).	Legal provision 176 / Article 88.2	*"In accordance with the* ***principle of proportionality*** *as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective."* This principle refers back to the TEU and the CFR.
	Article 5.3	*"The use of the 'real-time' remote biometric identification system concerned is* ***necessary for, and proportionate*** *to, achieving one of the objectives specified in paragraph 1, first subparagraph, point (h), as identified in the request and, in particular,* ***remains limited to what is strictly necessary..****"* Also applies to necessity criteria
	Article 44.3	*"Where a notified body finds that an AI system no longer meets the requirements set out in Section 2, it shall, taking account of* ***the principle of proportionality,*** *suspend or withdraw the certificate issued or impose restrictions on it, unless compliance with those requirements is ensured by appropriate corrective action taken by the provider of the system within an appropriate deadline set by the notified body."*
	Legal provision 33	*"..offence should be serious enough to potentially* ***justify the use*** *of 'real-time' remote biometric identification systems…"*
	Article 36.7 (e)	*"…that authority shall take the appropriate measures, where necessary,* ***to avoid a potential risk to health, safety or fundamental rights."***
	Legal provision 73	*"High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning,* ***ensure that they are used as intended****… "*
Legitimacy Legitimacy refers to the fact that the used technology	Legal provision 95	*"The use of post-remote biometric identification systems should be subject to safeguards. Post-remote biometric identification systems should always be used in a way that is* ***proportionate, legitimate and strictly necessary.."***



should be in line and prescribed within the law (Karliuk, 2022; Amnesty International, 2024)		Also refers to the criteria of proportionality, legitimacy and necessity.
	Legal provision 94	*Any processing of biometric data involved in the use of AI systems for biometric identification for the purpose of law enforcement needs to comply with Article 10 of Directive (EU) 2016/680, that allows such processing* ***only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data*** *subject and where authorised by Union or Member State law. Such use, when authorised, also needs to respect the principles laid down in Article 4 (1) of Directive (EU) 2016/680 including* ***lawfulness****, fairness and transparency,* ***purpose limitation****, accuracy and storage limitation"*
Necessity The used technology should be strictly necessary to achieve the goal (Karliuk, 2022; Amnesty International, 2024)	Legal provision 33	*"The use of those systems for the purpose of law enforcement should therefore be prohibited, except in exhaustively listed and narrowly defined situations,* ***where the use is strictly necessary to achieve a substantial public interest****, the importance of which outweighs the risks. ´* *".... recourse to 'real-time' remote biometric identification could, foreseeably, be* ***necessary*** *and* ***proportionate****...´*
	Legal provision 34	*"...remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be deployed only to confirm the specifically targeted individual's identity and* ***should be limited to what is strictly necessary****.."*
	Legal provision 35/ legal provision 70 / Article 5.3	*"..the use of the* ***AI system should be restricted to the absolute minimum necessary*** *and should be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself."*
	Legal provision 176	*"In accordance with the principle of proportionality as set out in that Article****, this Regulation does not go***

		beyond what is necessary in order to achieve that objective”
	Article 71.5	*“The EU database shall* ***contain personal data only in so far as necessary for collecting and processing information*** *in accordance with this Regulation.”*
	Article 78.5	*“The Commission* ***and Member States may exchange, where necessary****…,* ***confidential information with regulatory authorities of third countries*** *with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of confidentiality.”*
Appropriateness The used technology should be appropriate when achieving the goal (Karliuk, 2022; Amnesty International, 2024)	Legal provision 34	*“The reference database of persons should be* ***appropriate*** *for each use case in each of the situations mentioned above.”*
	Article 14.4-5	*“ For the purpose of implementing paragraphs 1, 2 and 3, the high-risk AI system shall be provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as* ***appropriate and proportionate…*** *“ For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 of this Article shall be such as to ensure that, in addition, no action or decision is taken by the deployer on the basis of the identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority.* ***The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control or asylum****, where Union or national law considers the application of this requirement to be* ***disproportionate****.”*
	Legal provision 35	*“..the use of the AI system should be restricted to the absolute minimum necessary and should be subject to* ***appropriate safeguards and conditions****, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself.”*

	Article 13	*"High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and* ***use it appropriately****.* …. *(vii) where applicable, information to enable deployers to interpret the output of the high-risk AI system and* ***use it appropriately****"*
	Article 19	*"Providers of high-risk AI systems shall keep the logs referred to in Article 12(1), automatically generated by their high-risk AI systems, to the extent such logs are under their control. Without prejudice to applicable Union or national law, the logs shall be kept for a period* ***appropriate to the intended purpose of the high-risk AI system.."***