Impact Assessment Requirements in the GDPR vs the AI Act: Overlaps, Divergence, and Implications

Tytti Rintamäki[a,*], Delaram Golpayegani[b], Dave Lewis[b], Edoardo Celeste[c], Harshvardhan J. Pandit[b,d,*]

[a]*ADAPT Centre, School of Computing, Dublin City University, Collins Ave Ext, Whitehall, Dublin, 9, Ireland*
[b]*ADAPT Centre, School of Computer Science & Statistics, Trinity College Dublin, O'Reilly Institute, Dublin, 2, Ireland*
[c]*ADAPT Centre, School of Law & Government, Dublin City University, Collins Ave Ext, Whitehall, Dublin, 9, Ireland*
[d]*AI Accountability Lab (AIAL), Trinity College Dublin, College Green, Dublin, 2, Ireland*

Abstract

Under the EU General Data Protection Regulation (GDPR), the processing of personal data with "new technologies", including Artificial Intelligence (AI), requires conducting a Data Protection Impact Assessment (DPIA) to evaluate potential risks to the rights and freedoms of individuals. In addition to identifying categories of processing that require a DPIA, the GDPR empowers national Data Protection Authorities (DPAs) to define additional categories where a DPIA is necessary. The recently adopted AI Act classifies AI technologies according to their level of risk to health, safety, and fundamental rights. For systems presenting high risk, the AI Act requires a Fundamental Rights Impact Assessment (FRIA) to be conducted, which represents an additional requirement for AI systems already subject to a DPIA under the GDPR. This context thus raises the question of how these two regulations work together and how their enforcement can be harmonised. This paper analyses DPIA requirements collected from all the 27 EU and 3 EEA countries which implement the GDPR, and compares them with the FRIA requirements defined in the AI Act. We show there are overlaps and divergences across national requirements to conduct impact assessments for the use of AI. Based on this, we argue for the need to harmonise the DPIA requirements across the EU/ EEA for an effective implementation of the GDPR, to improve the alignment with the AI Act, and to facilitate the sharing of risk assessment information earlier in the AI value chain to guide responsible innovation.

Keywords: AI Act, Data Protection Impact Assessment, DPIA, FRIA, Fundamental Rights Impact Assessment, GDPR, Impact Assessment

In the evolving landscape of Artificial Intelligence (AI), the interplay between technology and individual rights has become a focal point for all stakeholders, from policymakers and regulators to developers and users. As AI technologies are increasingly being integrated into our lives, ensuring that these systems align with fundamental rights and freedoms has become urgent. In the European context, the General Data Protection Regulation (GDPR) [1] and the recently published AI Act [2] are two regulatory frameworks which govern technologies and protect the

*Corresponding authors:
Email addresses: tytti.rintamaki@adaptcentre.ie (Tytti Rintamäki), me@harshp.com (Harshvardhan J. Pandit)

rights and freedoms of individuals [3]. The GDPR emphasises the protection of personal data and privacy, while the AI Act represents the first law in the world to comprehensively regulate AI. Despite their distinct scopes and objectives, they share a potentially significant overlap based on the role of personal data in developing and using AI systems [4].

The European regulatory landscape for digital technologies is elaborate, with significant overlap between the AI Act, GDPR, Data Governance Act, and Digital Services Act[5]. These frameworks protect fundamental rights and promote responsible digital practices through varying scopes. To encourage the reuse of data and enable data altruism, the Data Governance Act establishes frameworks that facilitate the sharing of data while requiring the assessment of risks and impacts of their intended use. The Digital Services Act focuses on online platforms and digital services, touching on issues raised in the GDPR, such as explanations of algorithms and transparency. Research has investigated areas of overlap and conflict between these regulations, specifically focusing on how to balance and comply with AI [3][5]. The GDPR addresses AI through provisions on automated decision-making, though it only prescribes requirements such as providing opt-outs and requiring human intervention in specific cases.

Impact assessments are instruments that regulations utilise to foster responsible innovation while tackling growing concerns such as fairness, harm, and upholding rights and freedoms. Article 35 of the GDPR requires a Data Protection Impact Assessment (DPIA) to be conducted for processing activities likely to result in a high risk to the rights and freedoms of natural persons. Similarly, Article 27 of the AI Act requires conducting a Fundamental Rights Impact Assessment (FRIA) for AI systems that are classified as 'high-risk' under Article 6 and Annex III. From this, it is evident that both the GDPR and the AI Act provide a framework for categorising activities as "high-risk" and have a requirement to assess their impact on rights and freedoms via DPIA and FRIA as instruments.

Even though the identification and categorisation of high-risk activities are central to both regulations, the GDPR and the AI Act have different scopes and authorities enforcing them, which increases the complexity of compliance for entities subject to both. Furthermore, the GDPR empowers countries via their nominated supervisory or Data Protection Authorities (DPAs) to produce their own list of processing activities that require conducting a DPIA. This gold-plating of uncoordinated additions to the GDPR is a hindrance to EU competitiveness [6] as it means the implementation of the GDPR across the EU is a cumbersome task both from the regulatory bodies perspective and the administrations within organisations navigating the law. Former EU Central Bank President Draghi highlighted the need to address such gold-plating phenomenon and subsequent inconsistencies in enforcement. This paper will address this key challenge by analysing the additional requirements imposed by the member states and assess the implications they pose to the effective implementation of the AI Act. Cases where AI systems utilise personal data are thus regulated under both the GDPR and the AI Act, and their categorisation as 'high-risk' depends on both regulations as well as the authorities and countries involved. Despite the increasingly large use of AI applications involving people and thus personal data, the AI Act does not dictate how its obligations should be interpreted alongside those from the GDPR, nor does it provide a mechanism for cooperation among their respective authorities. If left unexplored, this overlap between the GDPR and the AI Act will lead to regulatory uncertainties, delays in enforcement, and create economic barriers to innovation. Furthermore, despite seven years of GDPR enforcement, there have been no analyses of the variance in DPIA requirements across the EU/EEA, which means that the implementation of the AI Act is likely to be fragmented as entities scramble to understand how the use of AI is classified as 'high-risk' under each country's GDPR requirements. The study of overlap in high-risk classifications across both

the GDPR and the AI Act is therefore urgently required.

To address this important yet under explored overlap between the GDPR and the AI Act, we define the following research objectives to explore the intersections in the categorisation of high-risk technologies across the GDPR and the AI Act, as well as the implications of potential overlaps and divergences:

RO1 Identify the key criteria that determine high-risk processing activities in the GDPR and each Data Protection Authority's DPIA required lists (Section 2);

RO2 Identify where the GDPR applies and a DPIA is required for high-risk AI systems as defined in AI Act Annex III (Sections 3.1);

RO3 Compare high-risk categorisations in the the GDPR and the AI Act to identify overlaps, gaps, and variance (Section 3.2, 3.3, 3.4, 3.5);

RO4 Assess the implications of the finding of this work on the AI value chain regarding information sharing for high-risk categorisations and risk assessments (Section 4).

Our paper makes four novel contributions: (1) We provide a landscape analysis of the personal data processing activities requiring a DPIA across the GDPR, EDPB guidelines, and all 27 EU and 3 EEA countries; (2) We provide a framework to simplify high-risk categorisations under the GDPR and the AI Act based on criteria of the information required for the high-risk categorisations; (3) We identify which of AI Act's Annex III high-risk categorisations are subject to the GDPR's rules and when vice versa they are or can be categorised as high-risk under the GDPR; and (4) We describe how the obligations for conducting a DPIA under the GDPR, risk assessment and FRIA under the AI Act necessitate the sharing of information across the AI value chain - demonstrating how the impact of AI Act reaches upstream stakeholders i.e. those early in its development.

1. Background

The GDPR and the AI Act both employ risk-based approaches to protect fundamental rights and freedoms, yet their intersections remain largely unexplored in current literature. This gap is particularly significant as organisations developing or deploying AI systems processing personal data must navigate overlapping regulatory requirements, potentially including both Data Protection Impact Assessments (DPIAs) under the GDPR and Fundamental Rights Impact Assessments (FRIAs) under the AI Act. This section examines the existing risk assessment frameworks under both regulations, analyses current research on their alignment, and identifies critical gaps in understanding when and how these regulations' high-risk categorisations overlap or diverge. We first examine the GDPR's DPIA requirements and their implementation variations across EU Member States, then explore the AI Act's high-risk classification system, and finally review existing frameworks that attempt to bridge these regulatory requirements. Through this analysis, we establish the foundation for our novel contributions addressing the four research objectives outlined above: identifying key criteria for high-risk categorisation under both regulations, mapping their overlaps and divergences, and assessing implications for information sharing across the AI value chain.

1.1. The GDPR's Risk-Based Approach to Data Protection

Both the GDPR and the AI Act take risk-based approaches to protect rights and freedoms [7, 8]. In the GDPR, the assessment of the level of risk entails a binary classification (Article

35): high-risk and non-high-risk processing as the only two categorisations with the DPIA being an ex-ante or "preventative assessment" [9] and an obligation for data controllers to conduct when the processing of personal data is anticipated to pose risks to the rights and freedoms of individuals. Article 35 of the GDPR outlines the processing activities that require conducting a DPIA, with Article 35(1) using the term "new technologies" which is a technology-neutral and future-proof definition which today includes (innovative) AI technologies. Article35 states that a DPIA is required in three circumstances - first, when data processing involves automation for systematically and extensively evaluating natural persons and leads to 'legal effects'. Second, in case of large-scale processing of special categories (Article 9) or criminal convictions (Article 10). Third, in case of large-scale systematic monitoring of a publicly accessible area. In addition to these, the European Data Protection Board (EDPB) provides guidance for DPIAs using these criteria to identify nine conditions where a DPIA is required under the GDPR [10].

While the GDPR is a pan-EU regulation that requires consistent application, the practice of gold-plating, where Member States and their Data Protection Authorities (DPAs) expand the scope of an EU directive when incorporating it into national law, introduces variances in its implementation[6]. In regards to conducting Data Protection Impact Assessments, Article 35(4) authorises DPAs to compile lists of the processing activities that require a DPIA in their jurisdiction, leading to variances across jurisdictions. Prior work has demonstrated similar variance in the DPAs' templates provided for information to be maintained in Article 30 of the GDPR records of processing activities (ROPA) [11]. Such variances have impacts on the organisation's compliance activities, especially when the organisation is present or operates across member states or when data subjects from multiple member states are involved. To date, no work has explored the variance in DPIA requirements, i.e., what is considered high-risk across the countries that implement the GDPR.

Despite the DPIA being an important obligation in terms of its intent to protect rights and freedoms, there has been little exploration in the state of the art to build support systems that can enable an actor to identify when their activities are high-risk under the GDPR and require a DPIA, or what kinds of risks and impacts can be foreseen. Authoritative efforts such as CNIL's (the French DPA) Privacy Impact Assessment (PIA) software [12] that can create a knowledge base of shared risks to be used in a DPIA, or the ISO/IEC 29134:2023 guidelines for privacy impact assessments [13], do not explore the underlying question of what determines what is high-risk, which necessitates interpreting textual descriptions in laws on a case by case basis until suitable guidelines and case law are established. Therefore, based on prior similar work exploring the AI Act high-risk categorisations [14], it is necessary to create a framework to identify the 'key criteria' as the information necessary to identify when a DPIA is required, and use this to stimulate the creation of tools to help with regulatory processes [15] and to facilitate the comparison and alignment with the AI Act's high-risk categorisations.

1.2. EU AI Act's Risk Classification Framework

The AI Act adds a third category to the assessment of the level of risk mentioned earlier for the GDPR, specifically for unacceptable AI uses, which are prohibited ipso facto (Article 5) [8]. The AI Act defines risk as 'the combination of the probability of an occurrence of harm and the severity of that harm' (Article 3). The specific criteria for which applications are considered high-risk are defined in Annex I, which lists sectoral laws, and Annex III, which describes specific use-cases. For this paper, we focus on the high-risk systems listed in Annex III and exclude prohibited AI systems as these would require the interpretation of other sectoral laws [16].

Despite the importance of Annex III in determining high-risk status under the AI Act, there has been little analysis regarding its contents. Work by Golpayegani et al.[14] explored the clauses in Annex III and identified five key concepts whose combinations can be used to simplify the categorisation of high-risk applications. These five concepts represent (1) Domain or Sector, e.g. education; (2) Purpose, e.g. assessing exams; (3) Capability or involved AI technique, e.g. information retrieval; (4) AI Deployer, e.g. school; and (5) AI Subject, e.g. students. This framework of 5 concepts is useful to understand which information is required to assess whether an application is high-risk as per the Annex III clauses. The authors also provide taxonomies for each of the five concepts to support expressing practical use cases and the creation of automated tooling to support risk assessments.

We followed this approach and these concepts in our DPIA analysis (RO1) to compare the GDPR and the AI Act requirements regarding high-risk categorisation (RO2) and identified when the GDPR is applicable for Annex III clauses (RO3). Our research builds on the limited existing work examining the overlap between DPIAs and FRIAs. Notably, Thomaidou and Limniotis [4] identify several synergies between the two assessments, demonstrating that information required for a DPIA can be reused in a FRIA and vice versa. These synergies include data processing documentation, stakeholder involvement, impact on (fundamental) rights, and legal basis, supporting our proposal for a unified framework that streamlines risk evaluation for stakeholders managing AI systems.

1.3. State of the Art

Calvi and Kotzinos [17] discuss how assessments are required during different stages of a product's lifecycle across the regulations: GDPR's DPIA before personal data processing, AI Act's conformity assessment before introducing the AI system to the market, the Digital Services Act's risk assessments before deployment and the Fundamental Rights Impact Assessment before putting the system into use. They highlight areas of concern we are also looking at, namely how the different assessments address different risks, involve different entities and types of data, assign responsibility for the assessment differently and conduct them at different stages. We will discuss how this is further complicated by the nature of the AI value chain in Section 4, but we agree with the authors as they propose coordination to improve future policy choices. We believe that this could take the form of information sharing amongst the various assessments to assist upstream and downstream entities in their obligations.

Some countries have created frameworks and guidelines for trustworthy and responsible AI systems that build on the DPIA framework outlined in the GDPR in an AI-specific context. For example, CNIL released guidance on how to ensure the use of AI systems is compliant with the GDPR [18] with an emphasis on the development stage early in the life cycle - an area not covered by the AI Act itself. Their guides bridge the gap between the different regulatory frameworks, assisting in multiple aspects of the applicable legal regime. Regarding the GDPR, they assist in defining the purpose(s) of the system, defining controllers and processors, ensuring the lawfulness of processing, encouraging privacy by design and further assist in conducting a DPIA, amongst other things. Interestingly, CNIL discusses the risk criteria in the EU AI Act and takes the stance that all the high-risk systems listed in the Act will have to conduct a DPIA when personal data is involved. Our findings, detailed in this paper, show that the connection between the high-risk systems and guidance on when to carry out a DPIA is much more complicated, and there exists a difficulty in interpreting the conditions/criteria.

For entities carrying out these assessments, information sharing and coordination between them is necessary to have the required information for each assessment. For example, the Dutch

government's 2022 report [19] shows how the assessment of the impact on fundamental rights and freedoms can be based on the GDPR's DPIA. They utilised the process of identifying the objectives of data processing from DPIAs, but as the focus is on personal data, they concluded that much more needs to be added to account for the various elements involved in using algorithms. We utilised this argument about the usefulness of DPIA as a baseline for (RO4) to explore the implications of DPIA requirements on the AI Act across different stages of the AI value chain to reduce the burden for each entity in conducting their assessments and to ensure the appropriate enforcement of regulations.

Despite the considerable overlap in scope between the GDPR and the AI Act, current literature lacks a comprehensive framework for understanding when and how their high-risk categorisations intersect in practice. Whilst Thomaidou and Limniotis[4] identify potential synergies between DPIAs and FRIAs, and CNIL[18] assumes all AI Act high-risk systems will require DPIAs, no rigorous analysis exists documenting exactly which high-risk AI systems trigger DPIA requirements and under which specific jurisdictional conditions. This gap is particularly problematic given the significant variance in DPIA requirements across Member States—a variance that has remained unexplored in the academic literature despite its profound implications for cross-border AI deployment. Furthermore, existing research has not adequately addressed how these overlapping assessment requirements affect different actors across the AI value chain, nor how information must flow between these actors to enable compliance with both regulatory frameworks. Our research directly addresses this gap by providing the first systematic mapping of high-risk categorisations across both regulations, documenting jurisdictional variance in DPIA requirements, and analysing the practical implications for information sharing across the AI value chain.

2. Analysis of DPIA Required Criteria

2.1. Collecting DPIA Required Criteria Across EU/EEA Member States

A comprehensive assessment of high-risk processing activities and the necessity of conducting a DPIA requires consideration not only of the GDPR and the EDPB guidelines but also of the various lists issued by national Data Protection Authorities (DPAs). In order to identify the all conditions where a DPIA is necessary, we gathered all the processing activities listed in Article 35(3) of the GDPR, the guidelines published by the EDPB [10], and the lists of processing activities requiring a DPIA published by DPAs from all 27 EU and 3 EEA member states implementing the GDPR [20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49]. In accumulating these, we differentiated between pan-EU legally binding requirements (mentioned in the GDPR or by the EDPB) and those limited to specific jurisdictions/countries through their respective DPA lists. Due to varying national languages, only twelve out of the thirty guidelines were present in English. To ensure the documents were translated uniformly, we utilised the eTranslation service provided by the European Commission [50]. This neural machine translation service was trained using the past work of the EU institutions translators, amounting to over 1 billion sentences in 24 official EU languages. This meant it is particularly suited to translating EU documents in the various languages. After translating, we then identified each DPIA required condition (processing activity), and expressed it as a set of 'key concepts' (further described in Section 3.2) based on prior work applying similar techniques to the GDPR's Record of Processing Activities (ROPA) [11] and the AI Act's Annex III cases [51]. Essentially, taking the lengthy explanations from the guides and identifying what the processing activity is and expressing this as a condition. This analysis was done in the beginning of

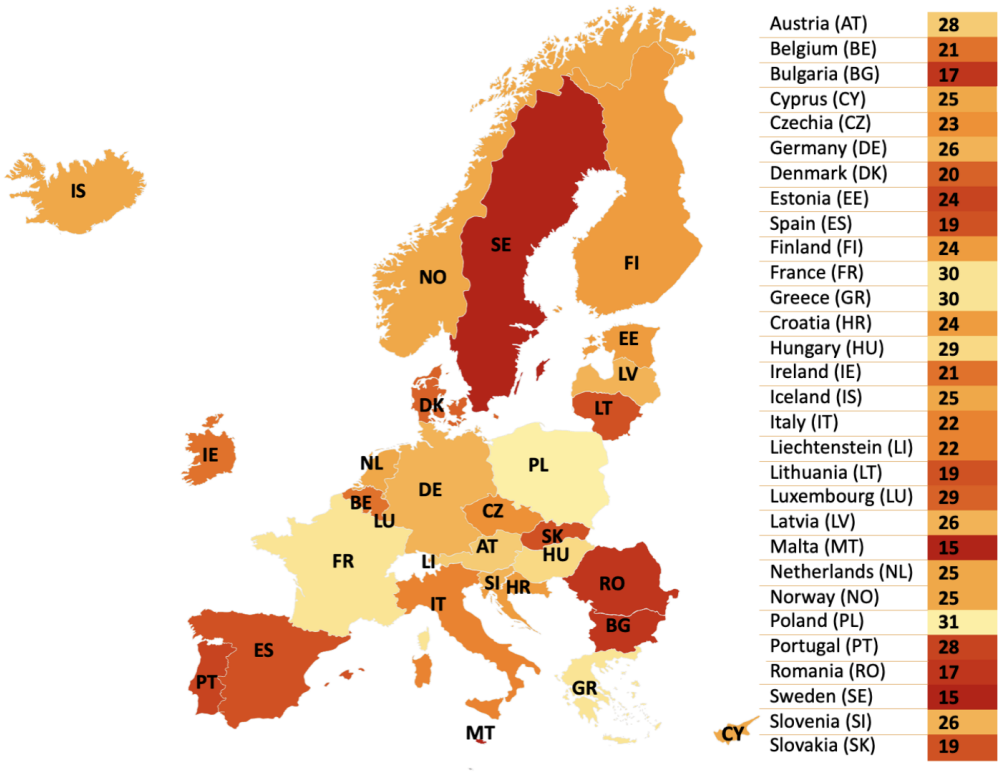

Figure 1: Number of processing activities requiring a DPIA by country (using ISO 3166-2 code). The colours convey the variance in regulatory requirements across the EU/ EEA, with dark red signifying the least amount of conditions requiring a DPIA and pale yellow requiring the most.

October 2025, taking into consideration any updates made by DPA's up until the 9th of October 2025.

Through this exercise, we compiled a list of exactly 114 distinct activities that represent all the DPIA-required conditions from the GDPR, EDPB, and member states' guidelines (provided at the end of this section). A visual representation of the variance in the amount of DPIA required conditions across the EU is shown in Figure. 1. Each member state is referred to by its ISO 3166-2 code, for example, 'AT' for Austria and 'FR' for France, with GDPR and EDPB noted first, followed by the member states in alphabetical order. This allows for a visual comparison of how many DPIA-required activities the data protection authorities in each country have defined in addition to those in regulatory guidelines. The number at the top of each bar indicates the total number of processing activities listed by the specific authority, for example, 30 activities listed by the Greek Data Protection Authority or 13 activities listed by the guidelines published by the EDPB.

Poland has the most conditions (n=31), followed by France and Greece (N=30). The least conditions are found in Sweden and Malta (n=15). The average number of conditions is around

22, a noticeable increase from the 10 listed in the GDPR or the 13 in EDPB's guidelines. Of note, the bulk of DPIA-required conditions in our list are from country-specific additions (101 out of 114). In these, the most common conditions include (large-scale) processing of communication and location data (23 countries), (large-scale) processing of employee activities (19 countries), and processing with legal effects such as access to or exclusion of services (12 countries). More specific activities such as large-scale processing of financial data (mentioned by 5 countries) and electronic monitoring at a school (mentioned by 2 countries) are more detailed and explicit processing activities as compared to other conditions. An interesting finding is that the use of any AI in processing requires a DPIA in Austria, Denmark, Germany, Greece, and the Czech Republic (5 countries) - *however these lists and the associated guidelines do not provide a legal definition of what should be considered as 'AI' - whilst the AI Act has its obligations based on a defined 'AI System' (Article 3). Both regulations thus assume that 'AI' is a well-established term and that it can be reasonably expected to identify when it is being used in an activity.*

The list below represents a few examples of the different processing activities requiring a DPIA by the GDPR, EDPB and the EU/EEA countries (defined using ISO 3166-2 codes). Each condition is expressed with a unique identifier "ID" (e.g. *C33*), followed by the statement describing the condition, and finally, sources which contain it. The complete list can be found in the Appendix A.

Table 1: Examples from List of DPIA Required Conditions

ID	**Type of Processing Activity**	**Authority requiring a DPIA**
C1	Large Scale processing of Special category personal data (Article 35(3b))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C2	Processing of Special Category of personal data for decision-making (Article 35(3b))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C3	Large scale purposes (Recital 91)	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C12	Processing of Genetic data	BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, LV, LI, LT, LU, MT, NL, NO, PL, PT, SK, SI, ES
C16	(Large scale) processing of employee activities	HR, CY, CZ, EE, FR, DE, GR, HU, IS, LV, LI, LT, LU, MT, NL, NO, PL, SK, SI
C32	Use of AI in processing	AT, CZ, DK, DE, GR
C33	Large scale processing in the context of fraud prevention	EE, FR, HU, NL

2.2. Key Criteria for Determining High-Risk Activities that Require a DPIA

We took the identified 114 conditions where a DPIA is requried from the GDPR, EDPB, and DPA lists, and identified their key criteria which determines whether the DPIA is required. These key criteria are described using information concepts such that providing these would be sufficient to identify whether the activity is high-risk according to which of the conditions it matches or satisfies. The concepts we identified in this manner were: (1) *Purpose* of processing activity; (2) *Personal Data* - especially whether it is sensitive or belonging to a special category, e.g. health data as per Article 9 of the GDPR or criminal convictions and offences as per Article 10 of the GDPR; (3) *Data Subjects* - especially whether they are vulnerable, e.g. children, minorities; (4) involvement of specific *Technology* - especially whether they are innovative and untested, e.g. AI; and (5) *Processing Context* - other relevant concepts such as involvement of automated decision making, profiling, and whether the processing produces *Impact*- especially whether the processing produces legal effects on the data subject, such as significant decisions or rights implications. Not all key concepts were required to express each high-risk condition. For example, according to Article 35(3b) of the GDPR, large-scale processing of special categories can be expressed as the combination of two concepts: processing context (large scale) and personal data (special categories).

3. Applicability of the GDPR and DPIA in AI Act's Annex III High-Risk Categorisations

3.1. Applicability of the GDPR to Annex III of the AI Act

Before analysing whether a DPIA is required, the activity must first be subject to the GDPR, i.e. it must involve the processing of personal data. Only after ascertaining this can we ask the question "When do high-risk AI systems involving risky (personal) data processing require a DPIA?". To do this, we identified where the following key concepts (from Section 3.2) are present in each high-risk condition defined in AI Act Annex III: (1) *Purpose* of the AI system ; (2) involvement of *Personal Data* - especially whether it is sensitive or special category; (3) the *(human) Subject* of the AI system - especially whether they are vulnerable; (4) possible involvement of specific *Technology* that triggers a DPIA - such as use of smart meters in Annex III-2a and (5) *Processing Context* - such as involvement of automated decision making, profiling, and (6) *Impact* whether the system produces legal effects for the subjects. In addition to describing where a condition is high-risk, some clauses also describe exemptions, such as III-5b, where the purpose is to detect financial fraud, or III-7a, for verification of travel documents. We also expressed such exceptions using the same key concepts so that in our later comparisons, we could distinguish and focus only on the high-risk categorisations. The output from this activity is presented at the end of 3.2. This exercise allowed us to understand which of the AI Act's Annex III high-risk conditions are subject to the GDPR based on the involvement of personal data and then identify where a DPIA is needed by matching the concepts with the representation of DPIA required conditions presented in the earlier section. We discuss these outcomes in the subsequent sections.

Expanding on the method to express high-risk conditions, this section provides detailed examples and explanations of how these concepts are used to interpret the applicability of the GDPR in AI Act's Annex III. First, we looked at information within the 25 high-risk descriptions in Annex.III (8 clauses and their sub-clauses) and assessed whether they involved personal data explicitly (i.e. it can be reasonably inferred from the description) or conditionally (i.e. it may potentially be involved in a specific application).

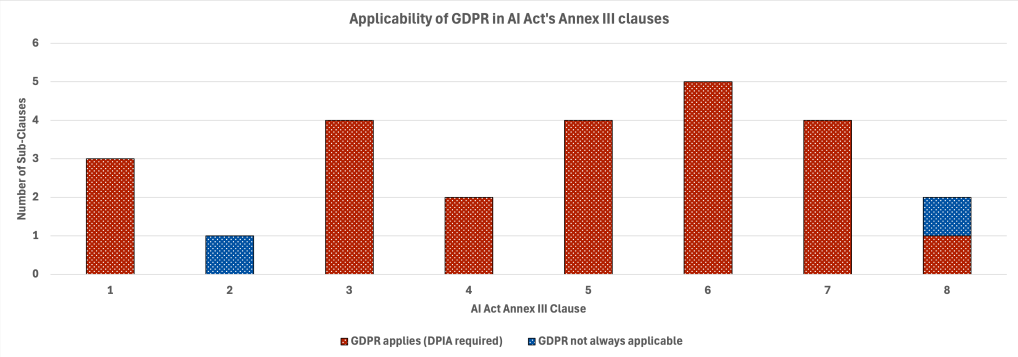

Figure 2: Applicability of the GDPR in the AI Act's Annex III clauses

From this exercise, we found **personal data is explicitly involved, and hence GDPR is applicable in 23 out of the 25 AI Act Annex. III clauses**, as shown in Figure 2. The remaining 2 cases where GDPR is not always applicable are Annex. III-2a and III-8a, where GDPR is conditionally applicable based on the involvement of personal data - which we found can reasonably arise in specific applications. Annex. III-2a concerns critical infrastructure where AI systems used as safety components in the management and operation of critical digital infrastructure, road traffic, and the supply of water, gas, heating and electricity. The type of data present in safety components of infrastructure management does not present a clear involvement of personal data. Similarly in Annex. III-8a concerning the use of AI systems in administration of justice and democratic processes, and intended to assist in researching and interpreting facts and the law, and in applying the law to a concrete set of facts - the explicit involvement of personal data being always present cannot be assumed.

However, in both cases, there is a reasonable foreseeable use-case where personal will be involved - for e.g. III-2a supply of electricity can involve personal data if it is to a private home, and III-8a can involve personal data when the process involves (information on) people. In addition to conditionally involving GDPR, investigating such conditional use-cases is also necessary to (later) assess where a DPIA could be required. For Annex. III-2a the use of smart meters in homes to measure the consumption of water, electricity and gas requires a DPIA in Hungary, Poland and Romania. For Annex. III-8a the process of researching and interpreting facts and the law where the system utilises data about criminal offences requires conducting a DPIA by the GDPR due to the involvement of a special category of personal data.

3.2. Determining When a DPIA is Required in AI Act Annex III Clauses

After identifying how the AI Act's Annex III high-risk activities involve personal data and hence will be regulated under the GDPR in 23 of the 25 clauses, and can conditionally involve GDPR in the remaining two, we sought to identify where a DPIA is required. To do this, we expressed each Annex III clause in terms of the identified key concepts (Personal Data, Purpose, Data Subject, Technology, and Processing Context), and then matched it with our collected corpus of 114 DPIA required conditions which reflect pan-EU/EEA requirements (from the GDPR and EDPB) and jurisdiction specific requirements (from DPA lists).

In this exercise, we found that each Annex III clause can have many distinct variations based on the key concepts involved (e.g. specific categories of personal data or technologies being used) such that a DPIA is required if certain conditions are met. To avoid further complexity of referring to explicit and conditional use-cases, and to enable better documentation of our findings, we distinguish such conditional use-cases through identifiers created by adding numeric suffixes to the Annex III clause numbers. For example, Annex III-2a involving critical infrastructure has three variations based on the involvement of smart meters (III-2a.1), road traffic video analysis (III-2a.2), and public transport monitoring systems (III-2a.3). Each such variation involves the conditional applicability of a concept (e.g. technology for III-2a) and allows us to match the Annex III clause to a DPIA-required condition, e.g. smart meters in III-2a.1 match with DPIA-required conditions from Hungary, Poland, and Romania.

In sum, we derived a total of 61 use-cases from the Annex III clauses, of which 25 reflect the Annex III's clauses and 36 are the additional use cases based on the conditional applicability of key concepts. For each of these 61 use-cases, we then identified whether there were any matching DPIA required conditions from the 114 collected conditions, and documented them by stating whether a DPIA is explicitly or always required or is conditionally required, and what the sources are for the conditions (i.e. whether it is required by the GDPR, EDPB, or a specific country). The outcome of this exercise is presented below.

The following list of a few examples expands on the GDPR concepts found in Annex III. Clauses with number/letter i.e. 1a, 2a, 3a, are the 25 clauses and sub-clauses found in Annex III. Clauses with identifiers of number/letter.numer. i.e. 2a.1, 3b.1 are the use cases we identified in our analysis that involve personal data and require conducting a DPIA by GDPR or individual member states. The remaining list can be found in the Appendix B.

Annex III 1a. Biometrics: An AI system intended to be used for the identification of people. This may produce legal or similarly significant effects on the subject, as the system could be used for access control, authentication, or other high-stakes decisions. The processing of biometric data, which is considered a special category of personal data under the GDPR, triggers the requirement for a Data Protection Impact Assessment (DPIA). This is due to the increased risks posed to individual rights and freedoms when processing such sensitive information. In addition to the GDPR DPIA requirement, many EU member states (AT, BE, BG, HR, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, LV, LI, LT, LU, MT, NL, NO, PL, PT, SK, SI, ES) have specific national Data Protection Authority guidelines mandating a DPIA for the processing of biometric data.

Annex III 3a. Education and Vocational Training: An AI system intended to be used for determining access/admission or assigning persons, utilising processing activities such as automated decision-making and profiling. This will produce legal effects on the subjects, as the AI-powered decisions could significantly impact an individual's educational or career opportunities. While this use case may not directly involve special category personal data, the automated decision-making and profiling activities still trigger the requirement for a DPIA under the GDPR and EDPB guidelines. Some EU member states (AT, CZ, DK, DE, GR) have additional national-level DPIA requirements specifically for the use of AI in processing personal data.

Annex III 3a.1. A use case for the above Annex III clause 3a involves determining access/admission or assigning persons, which utilises processing activities such as assessing or classifying natural persons, and systematic assessment of skills/competences/outcomes of tests/mental health/development. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, DE, LV, ES (Because of the use of the processing activity: Assessing or classifying of people), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 3a.2.A use case for the above Annex III clause 3a involves determining access/admission or assigning persons, which utilising processing activities such as automated decision-making, profiling, assessing or classifying natural persons, and systematic assessment of skills/competences/outcomes of tests/mental health/development. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, NL (student assessment), IE, IT, LT, MT, AT (Minors/vulnerable), AT, CY, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data) AT, CZ, DK, DE, GR (Due to the use of AI in processing).

3.3. Annex III Clauses Where a DPIA is Always Required Under the GDPR

For each of the 23 sub-clauses in AI Act Annex III where the GDPR is applicable, we found that all 23 of them require conducting a DPIA (based on conditions identified from the GDPR and EDPB guidelines). This means that **for 23 (of 25) sub-clauses in the AI Act's Annex III, conducting a DPIA is always mandatory**. For the remaining 2 sub-clauses, where the GDPR is conditionally applicable, a DPIA is also conditionally required when the condition matches the criteria from specific countries' DPIA required lists. This is visualised in Figure 2.

The requirement for DPIA in Annex III stem from two important criteria - the involvement of special categories of personal data and having a consequence/impact for the data subject that is considered as a 'legal effect' of significance. For involvement of special categories of personal data which require a DPIA under the GDPR, 10 out of the 25 sub-clauses in Annex III always require a DPIA and 15 conditionally require a DPIA based. In these, biometric data, which is relevant to assess AI Act prohibited practices such as those entailing facial recognition (Article 5(1e)), is involved in 3 sub-clauses explicitly (III-1a to c) and once conditionally (III-7d.1) for detecting, recognising or identifying natural persons in the context of migration, asylum and border control management. Health data is involved explicitly in one clause (III-5a) and six times conditionally (III-5c.2, III-5d.3, III-6b.1, III-7a.1, III-7b.1, and III-7c.3). Criminal offences data is involved in 2 sub-clauses explicitly (III-6a and III-6e) and 4 times conditionally (III-6a.3., III-6d.1b, III-6d.2 and III-8a.2) predominantly in the sector of law enforcement and once in the area of administration of justice and democracy.

For processing which impacts the subject by producing legal effects and thus requires a DPIA under the GDPR, 16 out of the 25 sub-clauses in Annex III produce legal effects for the data subjects, and the 9 remaining can conditionally produce legal effects in specific use cases. For example, Annex III-5b evaluates the creditworthiness of natural persons which is a legal effect based on the use of credit scores to determine access to services or benefits, and hence always requires a DPIA, as does Annex III-7c regarding systems used for the examination of applications for asylum, visa and residence permits produces legal effects as this will lead to decisions on the eligibility of individuals applying for the status and permits.

We also found that sectors explicitly mentioned in Annex III clauses, such as education, employment and law enforcement, correspond to those mentioned in the GDPR's DPIA required conditions published by most member states. This implies a necessity to further investigate whether these sectors can themselves be treated as being high-risk, which would make them a priority area for enforcement cooperation between the GDPR and the AI Act authorities.

3.4. Annex III Clauses Where a DPIA May be Required in Specific Countries

In addition to the conditions in Annex III clauses where a DPIA is always required under the GDPR and EDPB guidelines, we also explored whether any we could identify use-cases implied by the clause where a specific countries's DPIA required condition would apply. Since the GDPR is a pan-EU/EEA regulation, if a DPIA is required for any Annex III clause, then it is also required in all 30 EU/EEA member states. Therefore, we focused on the specific lists for activities requiring a DPIA published by DPAs from each country, and explored how and where they can be applicable for each clause in Annex III of the AI Act.

For this, we used the method in Section 3.2 where we created variations of the key concepts (Purpose, Personal Data, etc.) in a manner that would allow one or more of the 114 DPIA required conditions to be satisfied. Through this exercise, we created created additional 36 use-cases representing 22 clauses from Annex III-2 to III-8, and gave them identifiers (added

a numerical suffix to Annex clause number) to record our findings and aid in using them in discussions (e.g. III-2a.1 as described in Section 3.2).

We found at least one country that has a DPIA requirement for each of the 36 use-cases, which means that all except for III-1 where a DPIA is always required, each of the clauses from III-2 to III-8 has at least some reasonable scenario where a DPIA will be required. As mentioned earlier, the two clauses where the GDPR is not applicable i.e. III-2a regarding critical infrastructure and III-8a regarding justice processes, are the only two use-cases where a DPIA is neither always required by the GDPR, nor conditionally required under any country. However, we were able to identify specific use-cases by creating variations on the key concepts involved such that these clauses may also require a DPIA. Thus, **all 25 sub-clauses of the AI Act's Annex III have conditional use-cases which require a DPIA under one or more EU/EEA country**. This is illustrated in Figure 3.

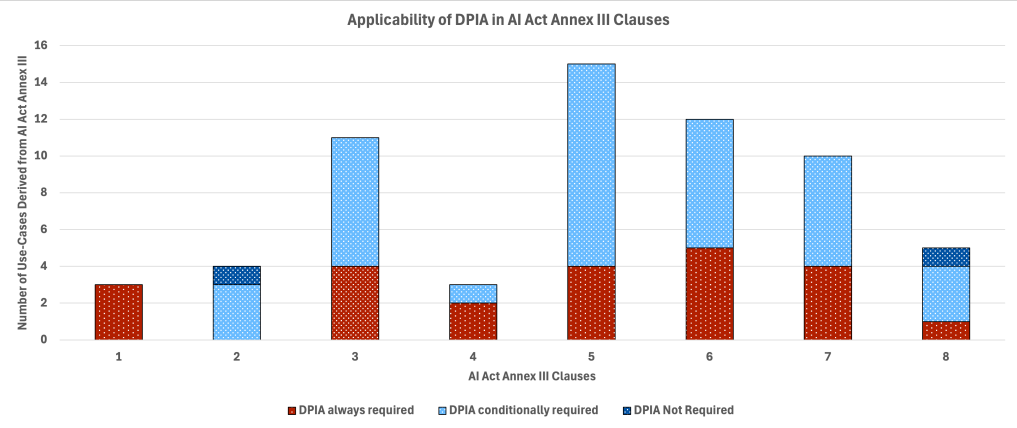

Figure 3: Analysis of 36 use-cases derived from the 25 clauses in Annex III of the AI Act, evaluating when a Data Protection Impact Assessment (DPIA) is required under the GDPR. Use-cases are categorised as those where a DPIA is always required, conditionally required based on foreseeable scenarios, or generally not required. For the two cases where a DPIA is not required, hypothetical scenarios were identified in which a DPIA could still be necessary. However, these are considered neither significant nor highly likely.

To illustrate the process of creating additional use cases for identifying where a DPIA is required, consider Annex III-5b.4. within which financial data is used to establish or assess the creditworthiness of individuals. Financial data or the processing activities required to establish creditworthiness do not align with any requirements in the GDPR or EDPB but is a type of personal data processing that requires conducting a DPIA by specific member states: Cyprus, Czech Republic, Estonia, Netherlands and Poland.

In the case of Annex III-8b, which involves AI systems used to influence the outcome of an election, referendum, or voting behaviour, a DPIA may be required based on whether special categories such as political opinions and religious or philosophical beliefs are involved. Processing of political opinions also explicitly requires a DPIA in 6 countries: Poland, Romania, Czech Republic, Finland, Italy, and Latvia. Poland specifically requires a DPIA where party affiliation and/or electoral preferences are involved. Belgium and the Netherlands, while not explicitly mentioning elections or voting, do require a DPIA when influencing the behaviour of natural

persons, which we presume takes place when influencing their voting behaviour.

Another example of sub-clauses where DPIA may be required is if the subject of the system belongs to a vulnerable group. This condition is present in 8 use-cases where this type of data may be involved (III-3a.2, III-3b.1, III-3c.1, III-3d.1, III-5b.3, III-5c.1, III-5d.2, III-6a.2). The vulnerable groups in these use-cases are minors, appearing mostly in the educational and private and public service sectors. Processing data of vulnerable persons is explicitly mentioned by 19 countries: Austria, Czech Republic, Germany, Spain, Finland, France, Hungary, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Malta, Norway, Portugal, Romania, Slovakia, Slovenia, Sweden; where minors are explicitly stated by 5 countries: Austria, Ireland, Italy, Latvia, and Malta. In multiple use-cases above, these minors are students as they are in the education sector, and processing their data for the purpose of assessment requires a DPIA in 2 countries: Hungary and the Netherlands. Thus, vulnerable data subjects requiring a DPIA is addressed by most countries (n=19) in various ways, with only some (n=10) of them taking into account the sectors where minors could be involved.

Several use-cases require a DPIA if they utilise either health data (III-5c.2. III-5d.3, III-6b.1, III-7a.1, III-7b.1, III-7c.3) or data related to criminal offences (III-6a.3, III-6d.1b, III-6d.2, III-8a.2) - which are special categories of personal data under the GDPR. Health data is only explicitly mentioned in the processing lists of 3 countries: Cyprus, the Netherlands and Poland. Criminal offences are mentioned in 4 use-cases and require a DPIA according to the GDPR as well as by 12 countries: Austria, Czech Republic, Estonia, Spain, Finland, Croatia, Latvia, Malta, Netherlands, Poland, Romania, Slovenia.

To show the outcome of our analysis, Table 2 shows the variance between member states in requiring a DPIA to be conducted for the 25 Annex III clauses and the 36 identified use-cases. The remaining continuations of this table that include the rest of the member states can be found in the Appendix C. Clauses of the form *number-letter* (e.g. 1a, 2a, 3a) are sub-clauses in Annex III, and the clauses with identifiers of the form *number-letter-number* (e.g. 2a.1., 3b.1) are the use cases we identified from the text of that clause. Highlighted rows in gray are the clauses from the text of the Annex III directly, and non-highlighted rows are the forseeable use-cases that we created by interpreting the clause based on variations in our identified key criteria e.g. for data subjects - involvement of minors. The use of '✓' denotes that '*Yes*' this regulation or member state requires conducting a DPIA for this (sub)clause or use case. The dash '-' signifies that there is no requirement to conduct a DPIA for this (sub)clause or use case.

Table 2: DPIA Applicability to Annex III and Identified Use-Cases according to the GDPR, EDPB and National Data Protection Authorities

AIA	GDPR	EDPB	AT	BE	BG	CY	CZ	DE	DK	EE	ES	FI
1a	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1b	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1c	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2a	-	-	✓	-	-	-	✓	✓	✓	-	-	-
2a.1	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
2a.2	✓	✓	✓	-	-	-	✓	✓	✓	-	-	✓
2a.3	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
3a	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	-
3a.1	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	-
3a.2	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
3b	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
3b.1	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
3c	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	-
3c.1	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
3d	✓	✓	✓	✓	-	-	✓	✓	✓	-	✓	-
3d.1	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
4a	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
4b	✓	✓	✓	✓	-	-	✓	✓	✓	-	✓	-
4b.1	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-
5a	✓	✓	✓	-	-	✓	✓	✓	✓	-	✓	✓
5b	✓	✓	✓	-	-	✓	✓	✓	✓	-	-	-
5b.1	✓	✓	✓	-	-	✓	✓	✓	✓	-	✓	✓
5b.2	✓	✓	✓	-	-	✓	✓	✓	✓	-	-	-
5b.3	✓	✓	✓	-	-	✓	✓	✓	✓	-	✓	✓
5b.4	✓	✓	✓	-	-	✓	✓	✓	✓	✓	-	-
5b.5	✓	✓	✓	-	-	✓	✓	✓	✓	-	-	-
5c	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
5c.1	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
5c.2	✓	✓	✓	-	-	✓	✓	✓	✓	-	✓	✓
5c.3	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	✓
5d	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
5d.1	✓	✓	✓	✓	-	-	✓	✓	✓	-	✓	-
5d.2	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
5d.3	✓	✓	✓	-	-	✓	✓	✓	✓	-	-	-
6a	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
6a.1	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
6a.2	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
6a.3	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓
6b	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
6b.1	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
6c	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓
6d	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
6d.1	✓	✓	✓	-	-	-	✓	✓	✓	-	-	-
6d.2	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
6d.3	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓
6e	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓
7a	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	-
7a.1	✓	✓	✓	-	-	✓	✓	✓	✓	✓	-	-
7b	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	-
7b.1	✓	✓	✓	-	-	✓	✓	✓	✓	✓	-	-
7c	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓
7c.1	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	-
7c.2	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	-
7c.3	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	-
7d	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	-
7d.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8a	-	-	✓	-	-	-	✓	✓	✓	-	-	-
8a.1	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓
8a.2	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓
8b	✓	✓	✓	✓	-	-	✓	✓	✓	-	✓	✓
8b.1	✓	✓	✓	✓	-	-	✓	✓	✓	-	-	✓
Total= 61	60	60	61	11	4	16	61	61	61	22	32	28

3.5. Variance in DPIA Required Conditions Across EU/EEA Member States

In addition to the GDPR's DPIA-required conditions, the 30 EU/EEA member states collectively have produced 93 distinct jurisdiction-specific requirements. This means that whether an activity should be considered high-risk under the GDPR depends not only on the GDPR itself - which is a pan-EU/EEA regulation - but also depends on the specific member states involved. This creates a variance in what is considered as 'high-risk' across the EU, and as a result, also in the level of safety and protection that a DPIA is intended to create. Such variances also complexities for organisations operating in specific jurisdictions, who face the burden of having to navigate and comply with jurisdiction-specific requirements, rather than producing a single compliance exercise that covers all of EU/EEA - which is not only economically feasible but also enables the organisation to operate in all covered jurisdictions. Further, since DPIAs are varied across EU/EEA, it creates ambiguities as organisations interacting with entities outside of their own jurisdictions cannot rely on a DPIA conducted by another entity as it would have used a different criteria for what is considered as 'high-risk' under the GDPR (and the local DPA).

Figure 4 provides a summarised view of this variance by showing the number of use-cases for each clause of the AI Act's Annex III where we identified that a country's DPIA requirement applies. It shows how some countries have a much higher number of DPIA required conditions that are aligned with specific clauses of the AI Act (e.g. III-1), while other clauses have little to no relevant DPIA required conditions across most countries (e.g. III-2, III-5). It also shows how some countries (e..g Austria (AT), Czechia (CZ), Germany (DE), Denmark (DK), and Greece (GR)) have DPIA required conditions that cover all the clauses, whereas others (e.g. Belgium (BE), Bulgaria (BG), Hungary (HR)) have very little coverage, and yet others (e.g. Luxembourg (LU), Latvia (LV), Malta (MT), Sweden (SE), Slovenia (SI)) have high coverage only for a specific clause (III-7).

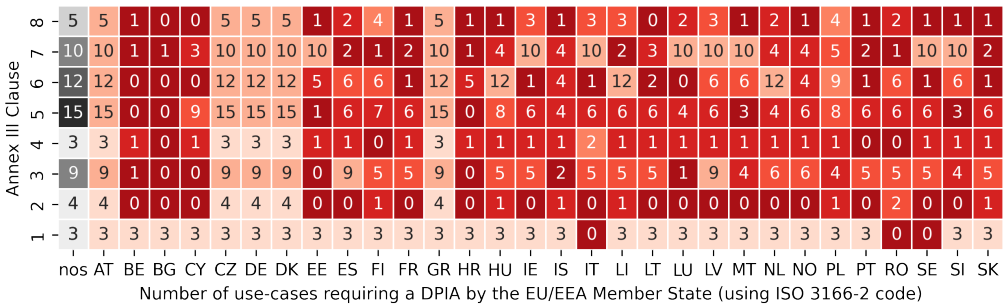

Figure 4: A heatmap showing the variance in EU/EEA Member States DPIA required conditions for AI Act's Annex III clauses. The numbers indicate how many of the identified use-cases for the Annex III clause (column '*nos*') satisfy a DPIA required condition from that country's GDPR Authority (higher numbers indicate significant overlap between the GDPR and the AI Act, while lower numbers indicate a lack of DPIA requirement for a high-risk activity in the AI Act.)

An example of the specific differences across member states is illustrated by the DPIA required conditions by DPAs in Hungary, Poland, and Romania which included smart meters used to measure (domestic) consumption in their guidelines. The authorities from these countries express their concerns regarding smart meters generating large-scale amounts of data by real-time sensors that convey it across the internet or other means. If using AI, this qualifies as high-risk

as per AI Act Annex III-2a regarding the supply of water, gas, heating and electricity. Other similar activities that also qualify under this clause are road traffic management in Austria and Poland, the use of tachographs in France, and the monitoring of road behaviour in Slovenia. This provides a clear indication to entities operating these types of AI systems within these jurisdictions that conducting a DPIA is legally necessary, but for other jurisdictions, the requirement to conduct a DPIA in these circumstances is not clear and is left up to their interpretation of the GDPR and relevant guidelines that may or may not recommend it.

A second example is Annex III-3b regarding monitoring and detecting prohibited behaviour of students during tests, for which 12 member states require a DPIA: Belgium, Austria, Czech Republic, Lithuania, Greece, Germany, Spain, Iceland, Norway, Latvia, Netherlands, and Denmark. The data processed for the use-cases mentioned in Annex III-3, there is a possibility that the subjects are minor (students in school), for which we found 10 countries that do not explicitly mention minors or vulnerable individuals/groups in their criteria for requiring a DPIA. This means there is an inconsistency in the level of data subject vulnerability requiring a DPIA between these 10 and the other 20 countries. In this, it is important to understand that our discussion is limited to the scope of the GDPR and its determination of what is 'high-risk', therefore even if there is existing national legislation and relevant case law that categorises minors as being vulnerable, our exercise stands to point out that there is a gap in acknowledging this within the DPIA required lists produced by specific countries.

A third example is Annex III-5c regarding risk assessment and pricing for life and health insurance, for which a DPIA is required in 5 countries: France, Greece, Italy, Poland, and Slovenia. Lastly, (only) France requires a DPIA for facilitating recruitment in employment which also qualifies as high-risk under Annex III-4a. Of interest, 5 member states specifically require conducting a DPIA when (any) AI is used in personal data processing: Austria, Czech Republic, Denmark, Germany and Greece, meaning a DPIA is required for any Annex III use case involving personal data processing taking which falls in scope of the DPA in these countries.

A final example is where the interpretation of DPIA requirements in Annex III is contingent upon the conditional use-cases in clauses such as III-2a critical infrastructure, III-3b AI systems intended to be used to evaluate learning outcomes and III-3d AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests. Some GDPR authorities have provided clarity on processing activities related to road safety and traffic management, but the interpretation of what constitutes as a safety component within a critical digital infrastructure remains open to debate.

Similarly, the classification of AI systems intended for educational purposes, such as monitoring student behaviour during tests, lacks consistent interpretations across jurisdictions. We found that if the data involved is of students that are underage, i.e. minors, a DPIA is required by the GDPR but otherwise requiring a DPIA assessment for the the evaluation and monitoring of the students varies by member states - and is highly dependent on the interpretation of whether these activities carry significant risks to the data subjects or constitutes a legal effect. Therefore, we highlight the urgent **necessity for consistency in guidance from the GDPR authorities which clarifies when and where a DPIA is required in Annex III use-cases**.

4. Implications of Findings for Risk Information Sharing Across the AI Value Chain

4.1. Legal Mechanisms and Obligations for Information Sharing

In the previous sections, we have demonstrated that variance across the EU/EEA member states exists for determining whether an activity requires a DPIA under the GDPR, and that this

variance also has a bearing on the high-risk categorisation under the AI Act. Impact assessments can be conducted at various points across the lifecycle of data and AI based value chains. However, while the GDPR focuses on regulating the processing of personal data, the AI Act seeks to regulate conformant products to be placed on the European Single Market under a common CE mark that offers assurances for protecting health, safety and fundamental rights based on the EU's New Legislative Framework. Thus the AI Act is most applicable at the product deployment and use stages, while the GDPR is applicable to all stages from the onset of AI development where (processing of) personal data is involved.

Article 27(4) of the AI Act allows the reuse of an existing DPIA to fulfil the obligations of FRIA. Further, Article 27(2) allows deployers that are public institutions or entities acting on their behalf to reuse the initial FRIA or rely on an existing FRIA from a provider for certain categories of AI systems listed in Annex III. This implies that the FRIA may be developed directly or indirectly in partnership between AI providers and deployers, as well as other entities who would have conducted a DPIA at earlier stages. With this, we have a mechanism where a DPIA conducted at the start or in the early stages of the AI value chain are shared downstream towards the later stages to culminate in a FRIA at product deployment and operation. Through this argument, we highlight that the determination of high-risk under the AI Act is an obligation that has consequences on the AI value chain beyond the immediate entity responsible for its implementation as it feeds requirements related to information sharing relevant for risk assessments back upstream to AI developers and other actors who are likely to have or support the downstream actors through their existing DPIA or by sharing the relevant information necessary to conduct a DPIA.

Based on this, we argue that cooperation should be sought in sharing DPIA, FRIA and other risk assessment information through formalised model clauses, such as those for AI public procurement contracts regarding high-risk AI which were published by the Commission in October 2023 [52]. These model clauses include the requirements for providers to document their risk management system but do not indicate that this should be linked to any specific requirement from the deployer arising from its initial FRIA or the option to offer an FRIA or DPIA as part of the risk assessment - though this document predated the final version of the Act which confirmed the FRIA requirement. Given that the Commission, specifically the AI Office as per Recital 143 and Article 63(3d), is charged with evaluating and promoting best practice in this area and creating a Code of Conduct as measures to support SMEs and start-ups, we suggest the development of appropriate guidelines that encourage sharing of DPIA and FRIA information across the product value chain.

Such an approach would be appropriate for challenges in AI risk management where various stages of the AI system development can be outsourced, triggering implications for the subsequent stages. The entity responsible for each stage would need to be fully informed of all decisions, responsibilities, risk mitigation strategies, errors, corrections, intentions and unforeseen issues that may have arisen across the value chain in the same way as if they would be fully informed had they completed the previous stages themselves. Without this understanding, entities are not equipped to make fully informed decisions when creating systems, which results in a lack of trust and transparency. Similarly, upstream developers and providers also benefit from receiving such information from entities using the developed products and services by way of providing an understanding of practical risks and impacts which can be addressed at earlier stages in the value chain [53].

Regulatory sandboxes can offer a suitable environment for evaluating flows of information arising from FRIA and DPIA obligations, potentially enhancing compliance efficiency through

information interoperability. This approach complements Article 27(5) of the AI Act, which mandates that the Commission's AI Office develop a template for a questionnaire that uses automation to facilitate the implementation of FRIA obligations. Given the research outlined in Section 2 and the notable parallels between DPIA and FRIA requirements- including their high-risk assessment criteria- the substantial work already completed on DPIA frameworks can be adapted to support FRIA systems. THe effectiveness of this adaptation could then be tested within specific member states under the existing GDPR regulatory sandbox mechanisms.

4.2. Impact of Variance in DPIA Requirements on AI Value Chain

The AI value chain consists of all actors, lifecycle stages, and processes involved in the planning, designing, development, deployment, and use of AI. The divergence for whether a processing activity or AI system is considered high-risk across regulations complicates the compliance procedures and creates a risk of inconsistent interpretations. This can lead to a regulatory environment that impacts organisations' compliance efforts, operational costs, and innovation, which makes it difficult to prevent and mitigate the harms arising from the use of AI. The common expected consequences from these are diverging high-risk classifications amongst actors, overlapping regulatory requirements, increased compliance costs and inconsistent enforcement across jurisdictions.

To discuss how this can happen, we use a hypothetical scenario, illustrated in Figure 5, where different across the AI Actors are subject to the GDPR and AI Act based on their specific use of personal data or AI systems, and have corresponding obligations to share information with other actors. We also depict practicalities outside legal obligations where organisations share information back to their developers and providers as part of market mechanisms which can be for service provision or as requirements for future product iterations.

In the scenario, the variance in member states' DPIA required lists creates ambiguities as to what is considered high-risk and thus where a DPIA would be created. As the actors are situated in different member states, the information they would retain regarding their DPIAs would be quite different from one another, which leads to fragmentation of information being shared across the value chain and a potential risk that crucial risk assessments needed or identified by one actor were never performed or considered by another actor both upstream and downstream from it. Further, as the DPIA is an important potential input for the FRIA obligations under the AI Act, a divergent DPIA that does not align with the actor conducting the FRIA can create a false sense of safety or gaps in risk assessments as information about specific measures earlier in the value chain would not be available.

Similarly, for actors earlier in the value chain to understand and respond to market needs and incidents at later stages, they must have a consistent knowledge of what risks and impacts can occur, and if an actor from a later stage wants to share their FRIA or DPIA, then it also risks repeating the same issues arising from the differences in what is considered high-risk across value chain stages. To further complicate matters, while the AI Act is relatively clear regarding the roles of actors at the end of the value chain - namely providers and deployers - the GDPR has a much more complex mechanism for assigning accountability through the criteria for determining a Controller (Article 4(7) of the GDPR). And since conducting a DPIA is the responsibility of a Controller (Article 35(1)), determining whether the activity constitutes as high-risk also depends on whether the actor correctly determines itself as a controller.

This can lead to strange arrangements, such as Controllers establishing themselves in jurisdictions that do not have sufficiently detailed high-risk categorisations for DPIA, thereby impacting not only the regulation of the GDPR, but also the AI Act by feeding in their potentially

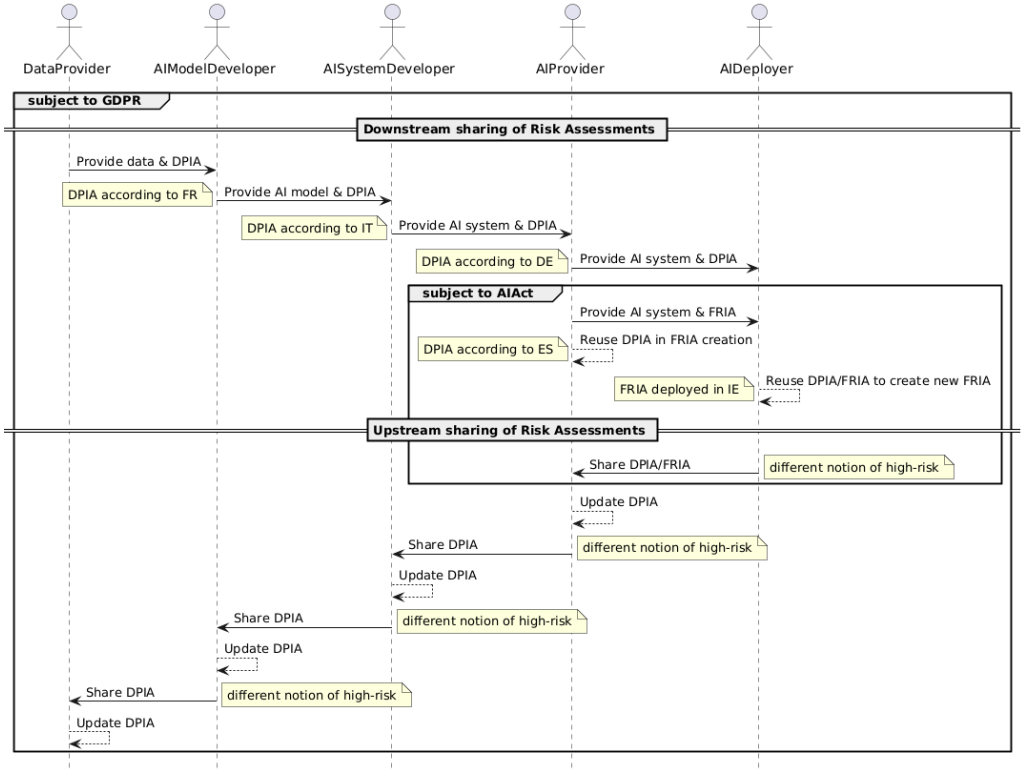

Figure 5: A hypothetical scenario showing the impact of variance in DPIA required conditions causing actors in different jurisdictions (expressed using ISO 3166-2 codes) to have different notions of high-risk regarding when a DPIA is needed, which ultimately affects the creation of FRIA towards deployment stages and also affects the sharing of (high) risk information back towards development stages

high-risk data and AI systems to actors at the end of the AI value chain who will now be burdened with increased risk management obligations. Similarly, AI Act actors might opt to certify their products in jurisdictions where it is less likely to be flagged as high-risk under the GDPR, and then use it across the EU/EEA market. Instead, if the GDPR and DPIA required conditions were harmonised, then their role in the AI Act's Annex III cases will also be streamlined, and a consistent interpretation and application of the GDPR and the AI Act's objectives regarding safeguarding the fundamental rights and freedoms, health, and safety will be upheld.

4.3. Overlaps Between DPIA and FRIA: Reusing One for the Other

When information is shared across the AI value chain, the time and resources taken to produce the various assessments is decreased, saving costs. This also has the positive effect of allowing other entities to use the information, limiting duplication of work and effort, and reducing mistakes with multiple eyes on the same information, therefore reducing the resources needed to meet the compliance requirement. The availability of such information can improve the speed of decision-making, as the information is centralised rather than needing to gather and

validate information from multiple sources, simultaneously increasing collaboration across departments. On a larger scale, it can lead to alignment with the national authorities responsible for issuing guidance to those operating in their jurisdiction and unburden data-driven models.

Information sharing can also play a crucial role in promoting responsible AI practices through enhancing ethical principles within organisations. Transparency is achieved when entities such as stakeholders have access to information, regardless of their position in the AI value chain. Accountability is strengthened through the availability of information, detailing decisions through which entities can be held accountable. The promotion of fairness and non-discrimination can be assisted through information sharing, as documenting the type of data and highlighting the potential risks involved can help inform downstream actors to identify and mitigate biases. In sum, this fosters informed risk assessments and inclusive decision-making by leveraging the collaborative involvement of different internal and external entities.

The DPIA and FRIA are ex-ante mechanisms, thus performed before the deployment of a personal data processing activity or an AI system. As explored above, a DPIA is expected to be involved much earlier in the AI development stages due to the scope of the GDPR, whereas the FRIA will occur at later stages closer to the deployment and use of the AI systems. Given the similarities between FRIA and DPIA [54], one of the critical questions in conducting FRIA revolves around its integration with existing impact assessments, in particular a DPIA. As AI Act Article 27(4) explicitly acknowledges the reuse of DPIA as a 'complement' to the FRIA obligations, understanding the extent to which an existing DPIA can be utilised to create and maintain a FRIA is of crucial interest.

However, this is complicated by the lack of clarity in AI Act Article 27(1a) regarding the interpretation of "a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose" in a manner that aligns with the GDPR's interpretation of "systematic description" in Article 35(7a) for a DPIA. Existing GDPR guidance states that this information involves the *nature* (e.g. sensitivity of data), *scope* (e.g. the scale of data and data subjects, frequency, and duration), and *context* (e.g. retention periods, security measures, and involvement of novel technologies) [10] of processing activities. Despite seemingly structured, these requirements for when a DPIA is to be conducted require a more nuanced categorisation of information, as evidenced by our analysis of all DPIA required conditions across EU/EEA and creating a framework for using it based on 'key concepts' which allowed us to identify gaps and align DPIA required conditions with the AI Act's high-risk categorisations.

We posit that further developing this framework and its key concepts would also be helpful to adapt an existing DPIA towards developing a FRIA by understanding which information in a DPIA fulfills which requirements for a FRIA. Based on this presumption, our analysis of DPIA requirements and its use to categorise Annex III use-cases should be useful in understanding how to explore the role of specific actors in the AI value chain who may be in control of or provide services associated with specific key concepts (e.g. providing technology such as facial recognition services), and developing appropriate mechanisms to share risk information from the earliest stages where it may simply exist as technical documentation to the latest stages where it takes the form of a DPIA and then a FRIA.

5. Conclusion

We started with the aim of understanding how the high-risk categorisations in the GDPR (defined through its DPIA obligations) and in the AI Act (defined and limited in our work to its Annex III clauses) align with each other, and what does this means for the application of both

the GDPR and the AI Act together within a high-risk use-case. We found that, to date, there has not been a comprehensive study for understanding the requirements to conduct a DPIA, despite its importance in upholding rights and freedoms. We therefore performed a remarkably comprehensive landscape analysis of all DPIA required conditions defined in the GDPR, in EDPB guidelines, and in the DPIA required processing activities published by Data Protection Authorities (DPAs) in all 30 EU/EEA member states where the GDPR applies. Through this, we showed the existence of 114 distinct conditions that define when a DPIA must be conducted and which have substantial variations in terms of applicability across the 30 EU/EEA member states. This finding provides sufficient evidence to request the EDPB to harmonise these DPIA required conditions, especially those affecting the interpretation and application of the GDPR with the AI Act, so as to provide for a smoother enforcement regime for both regulations.

Identifying and highlighting this variance is an important contribution as it not only reflects a divergence in the application of the GDPR across the EU/EEA, but also complicates the implementation of the AI Act as different use-cases have varying categorisations as high-risk across jurisdictions. To show this, we first analysed each of the 25 Annex III sub-clauses and showed that the GDPR always applies in 23 sub-clauses based on inherent processing of personal data. For the remaining 2 sub-clauses, we found plausible use-cases where the GDPR can conditionally apply. This is also an important contribution as despite both the GDPR and the AI Act being unprecedented major regulations, the drafting of the AI Act has had little acknowledgement of the applicability and reuse of the GDPR's existing obligations. By showing that the GDPR applies in 23 out of the 25 high-risk categories defined directly in the AI Act, we provide empirical evidence for their overlap and the necessity for their compliance and enforcement mechanisms and authorities to operate under close co-operation.

By reusing our analysis of DPIA required conditions, we also showed in the 23 sub-clauses of the AI Act's Annex III where the GDPR applies, a DPIA is also always necessary. This means that the development and use of high-risk AI systems under the AI Act in these cases will always be subject to the GDPR across EU/EEA - which has significant implications on the certification and compliance procedures for both regulations. Further, we also showed that the DPIA required conditions which vary across countries also create variances in how the AI Act's high-risk categorisations require a DPIA in some countries but not in others. This finding is significant for both the GDPR and the AI Act authorities as it exposes the potential for diverging safety standards across the EU/EEA single market based on where the AI system is developed and deployed. This finding is also important for the GDPR authorities to update their DPIA required guidance and processing lists to align better with the AI Act's Annex III use-cases.

Finally, we examined how variations in the GDPR's DPIA requirements impact both downstream development of FRIAs under the AI Act and upstream processes where additional DPIAs and risk assessments are needed. We explored these implications specifically in the context of similarities between FRIAs and DPIAs, and how these assessments influence information sharing across the AI value chain. Our findings indicate that effective information sharing can significantly benefit organisations internally, through optimised resource allocation, and externally by enhancing ethical AI practices. While the AI Act explicitly acknowledges the potential for reusing DPIAs in the FRIA process, our work demonstrates that such reuse depends on country-specific variations in DPIA requirements. Additionally, AI value chain actors must share their DPIAs at earlier stages to enable effective FRIA implementation later. This underscores the importance of identifying specific actors and their roles as controllers under the GDPR, as they bear the obligations to conduct and share DPIAs downstream for AI Act's compliance.

Our future work focuses on transforming these DPIA requirements into a machine-readable

format through our IMPACTO ontology. This ontology will encourage interoperability among organisations currently using varied methods to conduct their DPIAs and support future automation of this task. IMPACTO will contribute valuable concepts to the Data Privacy Vocabulary [55]. Our work has already informed the development of concepts to represent a FRIA, building upon existing DPIA frameworks [56], and the possibility of these to serve as information processes that support the development of automated tools [57]. We will also conduct a similar analysis of the prohibited AI systems under Article 5 of the AI Act, to determine how personal data is involved in these systems and whether emerging risks are accounted for in the GDPR. This will inform regulatory actions and harm prevention measures for data subjects specifically. We will investigate whether early development stages of prohibited systems qualify as high-risk under the GDPR's DPIA requirements despite falling outside the AI Act's scope. Similarly we will examine DPIA exemptions under the GDPR Article 35 and their variations across EU/EEA states, as this also has a bearing on the overlap between the GDPR amd AI Act. All this will inform our efforts on how risk information can effectively be shared across the AI value chain through DPIAs and FRIAS.

Funding Statement: This research was conducted with the financial support of Science Foundation Ireland under Grant Agreement No. 13/RC/2106_P2 at the ADAPT SFI Research Centre at Dublin City University and Trinity College Dublin. ADAPT, the SFI Research Centre for AI-Driven Digital Content Technology, is funded by Science Foundation Ireland through the SFI Research Centres Programme. Delaram Golpayegani has received funding through the PROTECT ITN Project from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant#813497. For the purpose of Open Access, the author has applied a CC-BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

Appendix A. List of Processing Activities Requiring a DPIA from the GDPR, European Data Protection Board and the EU member states and European Economic Area countries (in alphabetical order).

The Processing Activities requiring a DPIA Table (below) lists all the 114 identified processing activities considered to be high-risk and therefore require conducting a DPIA by the GDPR, EDPB and the EU member states and EEA countries (in alphabetical order.)

ID	DPIA Condition	Member States
C1	Large Scale processing of Special category personal data (Article 35(3b))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C2	Processing of Special Category of personal data for decision-making (Article 35(3b))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C3	Large scale purposes (Recital 91)	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C4	Profiling and/or processing of vulnerable persons data (Article 35(3b))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C5	Large scale Systematic monitoring of a publicly accessible area (Article 35(3c))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C6	Processing resulting in legal effects (Article 35(3a))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C7	(Large scale) profiling (Article 35(3a))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C8	Automated decision making and/or automated processing with legal or similar effect (Article 35(3a))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C9	Use of new technology or innovative use (Article 35(1))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C10	Large scale Processing of personal data relating to criminal offences or unlawful or bad conduct (Article 35(3b))	GDPR, EDPB, AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LT, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES, SE
C11	Processing of Biometric data	AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, LV, LI, LT, LU, MT, NL, NO, PL, PT, SK, SI, ES
C12	Processing of Genetic data	BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, LV, LI, LT, LU, MT, NL, NO, PL, PT, SK, SI, ES
C13	(Large-scale) Processing of communication and/or location data	AT, BE, BG, HR, CZ, EE, FI, FR, DE, GR, HU, IE, LV, LT, LU, NL, NO, PL, PT, RO, SK, SI
C14	Evaluation or scoring of individuals (including profiling or predicting)	EDPB, DK, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LU, NO, PL, PT, RO, SK, ES, SE
C15	Matching or Combining separate data sets/ registers	EDPB, AT, CY, CZ, DK, FI, DE, GR, HU, IE, IT, LV, LI, LU, NO, PL, SI, ES, SE
C16	(Large scale) processing of employee activities	HR, CY, CZ, EE, FR, DE, GR, HU, IS, LV, LI, LT, LU, MT, NL, NO, PL, SK, SI
C17	Processing resulting in Access to or exclusion of services	BE, HR, GR, IS, IT, LV, LI, NO, PL, SI, ES, SE
C18	Processing of data generated by devices connected to the Internet of things	HR, CY, GR, HU, IS, IT, NL, NO, PL, PT, RO, SI
C19	Processing intended to apply measurs to limit wholy or partly the rights or exercise of rights of data subjects	EDPB, CY, DE, GR, IT, LV, LI, LU, PL, SI, ES
C20	Profiling resulting in exclusion/suspension/rupture from a contract	BE, HR, FR, GR, IS, IT, LI, SI, ES, SE
C21	Processing data concerning asylum seekers	AT, IE, IT, LV, MT, SI, SE
C22	Processing of data revealing political opinions	CZ, FI, IT, LV, PL, RO
C23	The purpose of data processing is the application of 'smart meters' set up by public utilities providers (the monitoring of consumption customs).	BE, HR, GR, HU, NL, PL, RO

C24	Combining and/or matching data sets from two or more processing operations carried out for different purposes and/or by different controllers in the context of data processing that goes beyond the processing normally expected by a data subject, (provided that the use of algorithms can make decisions that significantly affect the data subject.)	AT, CZ, GR, IE, IT, LU, PL
C25	Processing operations aimed at monitoring, monitoring or controlling data subjects, in particular where the purpose is to influence them by profiling and automated decision-making.	BE, CY, DE, ES, FR, GR, HU, IT, NL, PT
C26	Processing of data for research purposes	AT, BE, CY, DE, FR, HU, IT, LU, MT, PT
C27	Processing data of children, including consent in relation to information society services	BE, CY, CZ, DE, FR, HU, IT, LV, PL, SE
C28	processing concerns personal data that has not been obtained from the data subject, and providing this information would prove difficult/ impossible	CZ, GR, IS, LV, LT, PT
C29	(credit score) The purpose of data processing is to assess the creditability of the data subject by way of evaluating personal data in large scale or systematically	CY, FR, HU, NL, SK, SI
C30	Processing of personal data for scientific or historical purposes where it is carried out without the data subject consents and together with at least one of the Criteria;	LV, LT, LU, NO, PT, SK
C31	Processing concerned with evaluating indivduals for various insurance purposes	FR, GR, IT, PL, SI
C32	Use of AI in processing	AT, CZ, DK, DE, GR
C33	Large scale processing in the context of fraud prevention	EE, FR, HU, NL
C34	Large scale processing of financial data	CZ, EE, NL, PL
C35	The processing of children's personal data for profiling or automated decision-making purposes or for marketing purposes, or for direct offering of services intended for them;	HR, HU, IS, LT, RO
C36	Use of facial recognition technology as part of the monitoring of a public–accessible area	DK, IT, PL, RO
C37	The use of new technologies or technological solutions for the processing of personal data or with the possibility of processing personal data to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of natural persons;	HR, DE, FI, HU, IS
C38	The processing of personal data by linking, comparing or verifying matches from multiple sources	HR, DE, LI, SI
C39	Large scale systematic processing of personal data concerning health and public health for public interest purposes as is the introduction and use of electronic prescription systems and the introduction and use of electronic health records or electronic health cards.	FR, GR, HU, NL
C40	Large scale data collection from third parties	GR, HU, IS, NO
C41	Processing of data used to assess the behaviour and other personal aspects of natural persons	AT, BE, HR, DE
C42	Health data collected automatically by implantable medical device	BE, IS, PT
C43	Processing operations aimed at monitoring, monitoring or controlling data subjects, in particular Roads with public transport which can be used by everyone	AT, FR, PL
C44	The processing of considerable amounts of personal data for law enforcement purposes.	HU, LI, NL
C45	Processing of personal data for the purpose of systematic assessment of skills, competences, outcomes of tests, mental health or development. (Sensitive personal data or other information reveals a sensitive nature and systematic monitoring).	IS, NO, PL
C46	Extensive processing of sensitive personal data for the purpose of developing algorithms	IS, IE, NO
C47	Extensive processing of data subject to social, professional or special official secrecy, even if it is not data pursuant to Article 9(1) and (10 GDPR)	EE, DE, LI
C48	Processing that involves an assessment or classification of natural persons	AT, HU, PL

C49	Use of a video recording system for monitoring road behaviour on motorways. The controller intends to use a smart video analysis system to isolate vehicles and automatically recognise their plates.	PL, SI
C50	Electronic monitoring at a school or preschool during the school/storage period. (Systematic and disadvantaged bodies).	IS, NO
C51	The purpose of data processing is to assess the solvency of the data subject by way of evaluating personal data in large scale or systematically	HU, SK
C52	where personal data are collected from third parties in order to be subsequently taken into account in the decision to refuse or terminate a specific service contract with a natural person;	BE, HR
C53	Processing of personal data of children in direct offering of information society services.	BG, LV
C54	Migration of data from existing to new technologies where this is related to large-scale data processing.	BG, DK
C55	(Systematic) transfer of special data categories between controllers	BE, NL
C56	Large-scale processing of behavioural data	BE, FR
C57	Supervision of the data subject, which is carried out in the following cases: a. if it is carried out on a large scale; b. if it is carried out at the workplace; c. if it applies to specially protected data subjects (e.g. health care, social care, prison, prison, educational institution, workplace).	LV, NL
C58	Large-scale tracking of data subjects	LV, LI
C59	Large-scale processing of health data	NL, PL
C60	Processing of personal data where data subjects have limited abilities to enforce their rights	CZ, SI
C61	Processing personal data with the purpose of providing services or developing products for commercial use that involve predicting working capacity, economic status, health, personal preferences or interests, trustworthiness, behavior, location or route (Sensitive data or data of highly personal nature and evaluation/scoring)	EE, FI, NO
C62	Innovate sensor or mobile based, centralised data collection	DE, SI
C63	Collection of public data in media social networking for profiling.	CY, PL
C64	Processing operations including capturing locations which may be entered by anyone due to a contractual obligation	AT
C65	Processing operations including recording places which may be entered by anyone on the basis of the public interest;	AT
C66	Processing operations including image processing using mobile cameras for the purpose of preventing or preventing dangerous attacks or criminal connections in public and non-public spaces;	AT
C67	Processing operations including image and acoustic processing for the preventive protection of persons or property on private residential properties not exclusively used by the person responsible and by all persons living in the common household	AT
C68	Processing operations including monitoring of churches, houses of prayer, as far as they are not already covered by lit. b and lit. e, and other institutions that serve the practice of religion in the community.	AT
C69	Camera Surveillance	NL
C70	Camera surveillance in schools or kindergartens during opening hours.	NO
C71	Processing operations carried out pursuant to Article 14 of the General Data Protection Regulation. If the information that should be provided to the data subject is subject to an exception under Article 14	SK
C72	Processing of presonal data with a link to other controllers or processors	CZ
C73	Large scale systematic processing of data of high significance or of a highly personal nature	GR

C74	The use of the personal data of pupils and students for assessment.	HU
C75	Processing operations establishing profiles of natural persons for human resources management purposes	FR
C76	Processing of health data implemented by health institutions or social medical institutions for the care of persons.	FR
C77	Investigation of applications and management of social housing	FR
C78	Treatments for the purpose of social or medico-social support for persons	FR
C79	File processing operations that may contain personal data of the entire national population,	LU
C80	Insufficient protection against unauthorised reversal of pseudonymisation.	IE
C81	When the data controller is planning to set up an application, tool, or platform for use by an entire sector to process also special categories of personal data.	HU
C82	Large scale systematic processing of personal data with the purpose of introducing, organizing, providing and monitoring the use of electronic government services	GR
C83	Processing of location data for the execution of decisions in the area of judicial¬enforcement	DK
C84	Processing of personal data in the context of the use of digital twins	DK
C85	Processing of personal data using neurotechnology	DK
C86	The processing of personal data using devices and technologies where the incident may endanger the health of an individual or more persons	HR
C87	where large-scale data is collected from third parties in order to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or displacement of natural persons	BE
C88	Processing of personal data carried out by a controller with a main establishment outside the EU	BG
C89	Regular and systematic processing where the provision of information under Article 19 of Regulation (EU) 2016/679	BG
C90	Processing operations in the personal area of persons, even if the processing is based on consent.	AT
C91	(Large-scale) Managing alerts and social and health reports or professional reports e.g. COVID-19	FR
C92	Processing using data from external sources	FR
C93	Anonymisation of personal data	DE
C94	Acquiring personal data where source is unknown	IE
C95	Processing of location data, including matching or combining datasets	FI
C96	Processing of location data concerning vulnerable data subjects	FI
C97	Processing of location data using systematic monitoring of data subjects	FI
C98	Processing of location data aimed at automated-decision making with legal or similar significant effect	FI
C99	Processing of location data when it prevents data subjects from exercising a right or using a service or a contracts	FI
C100	Processing of personal data in whistleblower systems	FI
C101	Large scale processing that might pose a risk of property loss (particularly in banking and credit card services)	EE
C102	Large scale processing that might pose a risk of violation of secrecy of correspondence (particularly in communication services)	EE
C103	Large scale processing that might pose a risk of identity theft or fraud (particularly in digital trust services and in comparable identity management services)	EE
C104	Large scale processing that might pose a risk of disclosure of personal economic standing (particularly taxation data, banking data, credit ranking data – publicly available data is not taken into account)	EE

C105	Large scale processing that might pose a risk of discrimination with legal consequences or with similar impact (particularly in labor broking services and in assessment/evaluation services that have impact on salaries and career)	EE
C106	Large scale processing that might pose a risk of loss of statutory confidentiality of information (restricted information, professional secrecy)	EE
C107	Combining special category data of filing systems	CY
C108	Processing activities for data breach notifications	CY
C109	Processing operations prior to the adoption of a law or a by-law	CY
C110	Transfer of special category data to a third country or to an international organisation	CY
C111	Application of CCTV	CY
C112	Applications offering users the possibility to store documents, emails, diaries, notes and very personal information from life-logging applications	CY
C113	Recording of telephone conversations	LT
C114	Processing of personal video data when video surveillance is conducted in areas not owned by the controller or healthcare settings or combined with sound recordings	LT

Appendix B. Identifying information for determining DPIA requirement in AI Act's Annex III

The following list expands on the GDPR concepts found in Annex III (Section 4.2-4.5 of this paper). Clauses with number/letter i.e. 1a, 2a, 3a, are the 25 clauses and subclauses found in Annex III. Clauses with identifiers of number/letter.numer. i.e. 2a.1, 3b.1 are the use cases we identified in our analysis that involve personal data and require conducting a DPIA by the GDPR or individual member states.

Below you will find descriptions that shows how personal data is involved in the high-risk AI systems listed in Annex III of the EU AI Act. These explanations were created by looking at information within the 25 high-risk descriptions (8 clauses and their subclauses) listed in Annex III, and assessing whether they involved personal data explicitly (i.e. it can be reasonably inferred from the description) or conditionally (i.e. it may be potentially involved in a particular application) to assess the applicability of GDPR to Annex III clauses. Similarly, for each of the key concepts we identified whether they are explicitly or conditionally applicable in each of the Annex III clauses. If a conditional applicability was identified, we added an identifier to distinguish the conditional clause from the main or explicit clause present in Annex III. Finally, we identified if the combination of the key concepts matched any of the DPIA required conditions identified from the analysis in Section 3. In this, we distinguished whether each condition came from the GDPR (i.e. GDPR Art.35 or EDPB) or a specific member state list - through which we determined whether the applicability of a DPIA required condition was uniform across the EU (i.e. it came from GDPR) or there was a variance (i.e. it is only present in one or more countries). From this exercise, we found personal data was explicitly involved and hence GDPR is applicable in 23 out of the 25 Annex III clauses as seen in the following table. The only ones where GDPR is not always applicable are Annex III clause 2a and clause 8a, though GDPR may be conditionally applicable based on the involvement of personal data in a particular use-case. To distinguish such conditional applicabilities, we created additional identifiers to distinguish between each variation, for example in Annex III-2a related to critical infrastructure we identified 3 variations based on involvement of: III-2a.1 smart meters, III-2a.2 road traffic video analysis, and III-2a.3 public transport monitoring systems. Each such variation involves the conditional applicability of a concept (technology for III-2a) and allows us to match the Annex III clause to a DPIA required condition, e.g. smart meters in III-2a.1 match with DPIA required conditions from Hun gary, Poland, and Romania. We found 36 such additional use cases based on the conditional applicability of key concepts in DPIA required conditions. In sum there are 61 total (sub)clauses and use cases for which a DPIA is always required for 21 use cases, is conditionally required for 38 and is not required for 2, as seen below.

Annex III 1a. Biometrics: An AI system intended to be used for the identification of people. This MAY produce legal effects on subjects, has the processing context of utilising remote processing, and involves special category personal data, specifically biometrics. A DPIA is required under the GDPR and EDPB guidelines due to the involvement of special category personal data, and in addition by member states: AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, LV, LI, LT, LU, MT, NL, NO, PL, PT, SK, SI, ES (due to involvement of Biometric data).

Annex III 1b. Biometrics: An AI system intended to be used for the identification of people. This MAY produce legal effects on subjects, processing context includes inferred data and profiling (categorisation), involves special categories of personal data, specifically biometrics, and data related to protected attributes or characteristics. A DPIA is required under the GDPR and EDPB guidelines due to the involvement of special category personal data, and in addition by member states: AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, LV, LI, LT, LU, MT, NL, NO, PL, PT, SK, SI, ES (due to involvement of Biometric data).

Annex III 1c. Biometrics: An AI system intended to be used for the identification of people. This MAY produce legal effects on subjects, processing context involves remote processing, involves special categories of personal data, specifically biometrics. A DPIA is required under the GDPR and EDPB guidelines due to the involvement of special category personal data, and in addition by member states: AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, LV, LI, LT, LU, MT, NL, NO, PL, PT, SK, SI, ES (due to involvement of Biometric data).

Annex III 2a. Critical Infrastructure: An AI system intended to be used for controlling the safety of critical digital infrastructure/road traffic/supply of water/gas/heating/electricity, which MAY produce legal effects on the subject. A DPIA is NOT required under the GDPR and EDPB guidelines, but is required by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 2a.1. A use case for the above Annex III clause 2a involves controlling the safety of critical digital infrastructure/road traffic/supply of water/gas/heating/electricity, by using smart meters to monitor individual household consumption and large-scale processing of personal data. This may produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines and in addition by member states: HU, PL, RO (Because processing activities include using smart meters), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 2a.2. A use case for the above Annex III clause 2a involves controlling the safety of critical digital infrastructure/road traffic/supply of water/gas/heating/electricity, specifically by using road traffic analysis and large-scale processing of personal data. This may produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT (Because processing activities include road traffic analysis), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 2a.3. A use case for the above Annex III clause 2a involves controlling the safety of critical digital infrastructure/road traffic/supply of water/gas/heating/electricity, by monitoring of public transport using large-scale processing of personal data. This may produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing), RO, SK (Because processing activities include monitoring of public transport).

Annex III 3a. Education and Vocational Training: An AI system intended to be used for determining access/admission or assigning persons utilising processing activities such as automated decision-making and profiling. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 3a.1. A use case for the above Annex III clause 3a involves determining access/admission or assigning persons, which utilises processing activities such as assessing or classifying natural persons, and systematic assessment of skills/competences/outcomes of tests/mental health/development. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, DE, LV, ES (Because of the use of the processing activity: Assessing or classifying of people), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 3a.2.A use case for the above Annex III clause 3a involves determining access/admission or assigning persons, which utilising processing activities such as automated decision-making, profiling, assessing or classifying natural persons, and systematic assessment of skills/competences/outcomes of tests/mental health/development. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, NL (student assessment), IE, IT, LT, MT, AT (Minors/vulnerable), AT, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data) AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 3b. Education and Vocational Training: An AI system intended to be used for evaluating learning outcomes, by utilising processing activities such as evaluation or scoring, systematic assessment of skills/competences/outcomes of tests/mental health/development. This will not produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: IS, NO, PL (Because of the use of the processing activity: assessment), DK, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LU, NO, PL, PT, RO, SK, ES, SE (Because of the use of the processing activity: evaluation or scoring), HU, NL (Due to the presence of student assessment processing activities), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 3b.1. A use case for the above Annex III clause 3b involves evaluating learning outcomes, by utilising processing activities: evaluation or scoring, and systematic assessment of skills/competences/outcomes of tests/mental health/development. This will not produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, NL (Due to the presence of student assessment processing activities), IE, IT, LT, MT, AT (Required because data specifically from minors is used), AT, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 3c. Education and Vocational Training: An AI system intended to be used for assessing appropriate level of education, and determining access, by use of processing activities such as automated decision-making, profiling, assessing or classifying natural persons, systematic assessment of skills/competences/outcomes of tests/mental health/development. This may produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 3c.1. A use case for the above Annex III clause 3c involves assessing the appropriate level of education and determining access, by use of processing activities such as automated decision-making, profiling, assessing or classifying natural persons, systematic assessment of skills/competences/outcomes of tests/mental health/development. This may produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, NL ((Due to the presence of student assessment activities), IE, IT, LT, MT, AT (Required because data specifically from minors is used), AT, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data).

Annex III 3d. Education and Vocational Training: An AI system intended to be used for monitoring/detecting prohibited behaviour of students during tests, utilises processing activities such as monitoring, surveillance, monitoring or controlling data subjects, electronic monitoring of a school, supervision of the data subject and uses behavioural data. This will not produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: BE, AT, CZ, DE, GR, LT, ES, IS, NO, LV, NL (Due to use of behavioural data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 3d.1. A use case for the above Annex III clause 3d involves an AI system that is intended to be used for monitoring/detecting prohibited behaviour of students during tests and utilises data from vulnerable data subjects, in this case, students who are minors. Processing activities utilised include monitoring, surveillance, monitoring or controlling data subjects, electronic monitoring of a school, supervision of the data subject and behavioural data. This will not produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, NL (Due to the presence of student assessment processing activities) IE, IT, LT, MT, AT (Required because data specifically from minors is used) AT, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data) BE, AT ,CZ, DE, GR, LT, ES, IS, NO, LV, NL (Due to use of behavioural data).

Annex III 4a. Employment, Workers Management, and Access to Self-Employment: An AI system intended to be used for recruitment and targeted job advertising, utilises processing activities such as automated decision-making, profiling, assessing or classifying natural persons, systematic assessment of skills/competences/outcomes of tests, and evaluation or scoring. This may produce legal effects

on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: FR (recruitment), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 4b. Employment, Workers Management, and Access to Self-Employment: An AI system intended to be used for promotion, termination, task allocation, monitoring, and evaluating, utilises processing activities such as automated decision-making, profiling, evaluation or scoring, monitoring of employee activities, exclusion/suspension/rupture from a contract, monitoring or controlling data subjects, providing services/developing products for commercial use that involve predicting working capacity/economic status/health/personal preferences/personal interests/ trustworthiness/ behaviour/ location/ route. It uses special category of data, specifically behavioural data. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: BE, AT, CZ, DE, GR, LT, ES, IS, NO, LV, NL (Due to use of behavioural data) AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 4b.1. A use case for the above Annex III clause 4b is an AI system intended to be used for promotion, termination, task allocation, monitoring, and evaluating, that utilises the processing activity of monitoring of employee activities, and uses behavioural data. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: BE, HR, CZ, EE, DE, GR, HU, IS, LV, LI, LT, LU, MT, NL, NO, SK, CY, IT, SI, ES, SE, AT (Because of the use of the processing activity: monitoring of employee activities) AT, CZ, DK, DE, GR (Due to the use of AI in processing) BE, AT, CZ, DE, GR, LT, ES, IS, NO, LV, NL (Due to use of behavioural data).

Annex III 5a. Access to essential private and public services and benefits: An AI system intended to be used for evaluating eligibility for and managing benefits and services, and utilises processing activities such as automated decision-making and profiling (categorization), and special category personal data, specifically health data, and protected attributes or characteristics including public service eligibility. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: CY, NL, PL, (Required as health data is used), FI, FR, HU, IS, IE, IT, LV, LI, LU, NO, PT, RO, SK, ES, SE (Because of the use of the processing activity: evaluation or scoring) AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5b. Access to essential private and public services and benefits: An AI system intended to be used for establishing or assessing/evaluating creditworthiness, involves processing activities such as profiling, evaluation or scoring, and includes special categories of personal data such as financial data, and protected attributes or characteristics included in creditworthiness evaluation. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: NL, SI, SK, HU, FR, CY (Because of the use of the processing activity: establishing credit score) PL, NL, CZ, EE (Required as financial data is used), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5b.1 A use case for the above Annex III clause 5b involves processing activity of evaluation or scoring and produces legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: NL, SI, SK, HU, FR, CY (Because of the use of the processing activity: establishing credit score) DK, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LU, NO, PL, PT, RO, SK, ES, SE (Because of the use of the processing activity: evaluation or scoring) AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5b.2. A use case for the above Annex III clause 5b involves the processing activity of assessing or classifying natural persons. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: NL, SI, SK, HU, FR, CY (Because of the use of the processing activity: establishing credit score) PL, AT, HU (Because of the use of the processing activity: assessing or classifying people) AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5b.3. A use case for the above Annex III clause 5b utilises processing activities such as profiling, evaluation or scoring, assessing or classifying natural persons, and activities to establish credit score utilises financial data and personal data of vulnerable persons is used. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: NL, SI, SK, HU, FR, CY (Because of the use of the processing activity: establishing credit score) AT, CZ, DK, DE, GR (Due to the use of AI in processing) AT, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data).

Annex III 5b.4. A use case for the above Annex III clause 5b involves financial data and produces legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: PL, NL, CZ, EE (Required as financial data is used) NL, SI, SK, HU, FR, CY (Because of the use of the processing activity: establishing credit score) AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5b.5. A use case for the above Annex III clause 5b involves processing data to establish individual credit scores. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing) NL, SI, SK, HU, FR, CY (Because of the use of the processing activity: establishing credit score).

Annex III 5c. Access to essential private and public services and benefits: An AI system intended to be used for life and health insurance pricing and risk assessment utilises processing activities: evaluation or scoring, assessing or classifying natural persons and profiling. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, HU, PL (Due to processing for insurance purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5c.1. A use case for the above Annex III clause 5c involves processing activities such as evaluation or scoring, assessing or classifying natural persons and profiling. It utilises financial data, and data of vulnerable persons. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, HU, PL (Due to processing for insurance purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing), CY, DK, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LU, NO, PL, PT, RO, SK, ES, SE (Because of the use of the processing activity: evaluation or scoring) AT, CY, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data).

Annex III 5c.2. A use case for the above Annex III clause 5c involves an AI system intended to be used for life and health insurance pricing and risk assessment and utilises health data to do so. This utilises processing activities such as evaluation or scoring, assessing or classifying natural persons and profiling. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, HU, PL (Due to processing for insurance purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing), CY, NL, PL (Required as health data is used), DK, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LU, NO, PL, PT, RO, SK, ES, SE (Because of the use of the processing activity: evaluation or scoring).

Annex III 5c.3. A use case for the above Annex III clause 5c involves financial data and produced legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: CZ, EE, NL, PL (Required as financial data is used), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5d. Access to essential private and public services and benefits: An AI system intended to be used to evaluate and classify emergency calls, dispatch or establish priority for dispatching emergency first response services, utilises processing activities such as automated decision making and evaluation or scoring. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5d.1. A use case for the above Annex III clause 5d utilises processing activities such as evaluation or scoring and results in exclusion/ access to services. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: BE, HR, GR, IS. IT, LV, LI, NO, PL, SI, ES, SE (Because processing results in exclusion/ access to services) AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 5d.2. A use case for the above Annex III clause 5d utilises processing activities such as automated decision making, evaluation or scoring, and results in exclusion/access to services, and uses vulnerable persons data. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing), AT, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data).

Annex III 5d.3. A use case for the above Annex III clause 5d involves an AI system intended to be used for evaluating and classifying emergency calls, dispatching or establishing priority for dispatching emergency first response services and utilises health data to do so. This utilises processing activities such as automated decision-making, evaluation or scoring and results in exclusion/access to services. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: CY, NL, PL (Required as health data is used), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 6a. Law enforcement: An AI system intended to be used for assessing the risk of becoming victims of criminal offences utilises processing activities such as profiling and assessing or classifying natural persons. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing), HU, LI, NL (Because of processing personal data for law enforcement purposes), IS, NO, PL, AT, HU (Because of the use of the processing activity: assessing or classifying people).

Annex III 6a.1. A use case for the above Annex III clause 6a involves the processing activity of assessing or classifying natural persons. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: IS, NO, PL, AT, HU (Because of the use of the processing activity: assessing or classifying people), AT, CZ, DK, DE, GR (Use of AI in processing), HU, LI, NL (Because of processing personal data for law enforcement purposes).

Annex III 6a.2. A use case for the above Annex III clause 6a involves the processing activity of profiling and assessing or classifying natural persons, specifically for vulnerable persons. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing), IS, NO, PL, AT, HU (Because of the use of the processing activity: assessing or classifying people), AT, CZ, DE, ES, FI, FR, HU, IE, IT, LV, LI, LT, MT, NO, PT, RO, SK, SI, SE (Because of the use of Vulnerable data subject data).

Annex III 6a.3. A use case for the above Annex III clause 6a involves large-scale processing of personal data relating to criminal offences or unlawful or bad conduct (Article 35(3b)), criminal offences, YES. DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing), IS, NO, PL, AT, HU (Because of the use of the processing activity: assessing or classifying people), AT, CZ, EE, ES, FI, HR, LV, MT, NL, PL, RO, SI (Required as data related to criminal offences is used).

Annex III 6b. Law enforcement: An AI system intended to be used for information verification in questioning, which produces legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 6b.1. A use case for the above Annex III clause 6b involves an AI system intended to be used for information verification and utilises health data to do so. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: NL, PL (Required as health data is used), HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 6c. Law enforcement: An AI system intended to be used for evaluating the reliability of evidence in the investigation and evaluating the reliability of evidence in criminal prosecution. This utilises processing activities such as, large scale processing of personal data relating to criminal offences or unlawful or bad conduct (Article 35(3b)), and data related to criminal offences. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing), AT, CZ, EE, ES, FI, HR, LV, MT, NL, PL, RO, SI (Required as data related to criminal offences is used).

Annex III 6d. Law enforcement: An AI system intended to be used for assessing the risk of offending, assessing the risk of re-offending, and assessing personality traits. This utilises processing activities such as profiling, assessing past criminal behaviour of individuals/groups, large-scale processing of personal data relating to criminal offences or unlawful or bad conduct (Article 35(3b)), and data related to personality traits/characteristics. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 6d.1. A use case for the above Annex III clause 6d involves assessing the risk of offending. This utilises processing activities such as profiling and uses data related to racial or ethnic origin, political opinions, and religious or philosophical beliefs. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 6d.1b. A use case for the above Annex III clause 6d involves assessing past criminal behaviour. This utilises processing activities such as large scale processing of personal data relating to criminal offences or unlawful or bad conduct (Article 35(3b)), and processing of data related to criminal offences. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing), AT, CZ, EE, ES, FI, HR, LV, MT, NL, PL, RO, SI (Required as data related to criminal offences is used).

Annex III 6d.2. A third use case for the above Annex III clause 6d involves assessing risk of offending, assessing risk or re-offending, assessing personality traits. This utilises processing activities such as assessing personality traits/characteristics, using behavioural data, behaviour or other personal aspects of natural persons, and data related to criminal offences. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing), AT, CZ, EE, ES, FI, HR, LV, MT, NL, PL,

RO, SI (Required as data related to criminal offences is used) BE, AT, CZ, DE, GR, LT, ES, IS, NO, LV, NL (Due to use of behavioural data).

Annex III 6e. Law enforcement: An AI system intended to be used for profiling for the detection, investigation, or prosecution of criminal offences. This will involve processing activities such as profiling, large-scale processing of personal data relating to criminal offences or unlawful or bad conduct (Article 35(3b)), and processing of data related to criminal offences. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: HU, LI, NL (Because of processing personal data for law enforcement purposes), AT, CZ, DK, DE, GR (Due to the use of AI in processing), AT, CZ, EE, ES, FI, HR, LV, MT, NL, PL, RO, SI (Required as data related to criminal offences is used).

Annex III 7a. Migration, asylum and border control management: An AI system intended to be used for information verification in questioning, which MAY produce legal effects on the subject. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 7a.1. A use case for the above Annex III clause 7a involves an AI system intended to be used for information verification and utilises health data to do so. This may produce legal effects on the subject. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: CY, NL, PL (Required as health data is used), SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 7b. Migration, asylum and border control management: An AI system intended to be used for assessing risk, security risk, risk of irregular migration, health risk. This will produce legal effects and involve processing activities such as assessing or classifying natural persons and profiling. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, HU, PL, NL, IS, NO (Because of the use of the processing activity: assessing or classifying people), SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 7b.1. A use case for the above Annex III clause 7b that involves assessing health risk includes processing activities such as assessing or classifying natural persons and profiling. It will utilise special category personal data, specifically health data and produce legal effects on the subject. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: CY, NL, PL (Required as health data is used), AT, HU, PL, NL, IS, NO (Because of the use of the processing activity: assessing or classifying people), SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 7c. Migration, asylum and border control management: An AI system intended to be used for examining asylum applications, visa, and residence permits which utilises processing activities such as evaluation or scoring, automated decision making, assessing or classifying natural persons and profiling. This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing), DK, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LU, NO, PL, PT, RO, SK, ES, SE (Because of the use of the processing activity: evaluation or scoring).

Annex III 7c.1. A use case for the above Annex III clause 7c is an AI system intended to be used for examining complaints related to asylum applications, visa and residence permits, which produces legal effects on subjects. ADPIA is required under the GDPR and EDPB guidelines, and in addition by member states: SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 7c.2. A second use case for the above Annex III clause 7c is an AI system that is intended to be used on assessing reliability of evidence, and may produces legal effects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 7c.3. A third use case for the above Annex III clause 7c is one that involves health data (e.g., when someone applies for a medical treatment visa), sensitive data (e.g., sexual orientation for LGBTQ+ asylum seekers or political opinion for those seeking protection). This will produce legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 7d. Migration, asylum and border control management: An AI system intended to be used for detecting, recognizing, or identifying natural persons. This produces legal effects and involves profiling. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 7d.1. A use case for the above Annex III clause 7d involves profiling, biometric data, and produces legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: SE, AT, IE, IT, LV, MT, SI (Because of the use of Asylum seekers data), AT, BE, BG, HR, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IS, IE, LV, LI, LT, LU, MT, NL, NO, PL, PT, SK, SI, ES (Involvement of Biometric data), AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 8a. Administration of justice and democratic processes: An AI system that involves researching and interpreting facts and the law; applying the law to facts; applying facts for dispute resolution. The system will produce legal effects on the subject. The organisation/ agent involved includes judicial authorities and judicial authority agents. A DPIA is NOT required under the GDPR and EDPB guidelines, but is required by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Annex III 8a.1. A use case for the above Annex III clause 8a involves the processing context of evaluation or scoring, profiling, and automated decision-making. The system will produce legal effects on the subject. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing), DK, FI, FR, DE, GR, HU, IS, IE, IT, LV, LI, LU, NO, PL, PT, RO, SK, ES, SE (Because of the use of the processing activity: evaluation or scoring).

Annex III 8a.2. A use case for the above Annex III clause 8a involves the use of personal data about criminal offences, produces legal effects on the subject. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: AT, CZ, DK, DE, GR (Due to the use of AI in processing), AT, CZ, EE, ES, FI, HR, LV, MT, NL, PL, RO, SI (Because of personal data about criminal offences).

Annex III 8b. Administration of justice and democratic processes: An AI system that involves influencing the outcome of an election or referendum; produces legal effects on the subject and involves special category personal data, specifically behavioural data. A DPIA is required under the GDPR and EDPB guidelines, and in addition by member states: PL (Processing by public authorities or private parties of personal data relating to party affiliation and/or electoral preferences) BE, AT, CZ, DE, GR, LT, ES, IS, NO, LV, NL (Behavioural data).

Annex III 8b.1. A use case for the above Annex III clause 8b, is an AI system that involves personal data about political opinions which produces legal effects on subjects. A DPIA is required under the GDPR and EDPB guidelines due to the presence of political opinion data. In addition, a DPIA is required by member states: PL (Data about political opinions)RO, CZ, FI, IT, LV (Because of processing by public authorities or private parties of personal data relating to party affiliation and/or electoral preferences), BE, NL (as processing may Influence behaviour of subjects) and AT, CZ, DK, DE, GR (Due to the use of AI in processing).

Appendix C. DPIA requirements in AI Act's Annex III clauses for each EU/EEA Member State

This table shows the variance between member states in requiring a DPIA to be conducted for the 25 Annex III clauses and the 36 identified use-cases. Clauses with number/letter i.e. 1a, 2a, 3a, are the 25 clauses and subclauses found in Annex III, and the clauses with identifiers of number/letter.numer. i.e. 2a.1., 3b.1. are the use cases we identified in our analysis that involve personal data and require conducting a DPIA by the GDPR or individual member states. Highlighted rows represent the direct interpretation of the use cases as mentioned in the Annex III clause, and non-highlighted rows are forseeable use-cases within the clause based on a specific condition e.g. involvement of minors - based on Appendix B. The use of "✓" in a cell denotes that "Yes" this member state requires conducting a DPIA for this (sub)clause or use case. The dash "-" signifies that there is no DPIA requirement for this (sub)clause or use case.

AIA	GDPR	EDPB	FR	GR	HR	HU	IE	IS	IT	LI	LT	LU
1a	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓
1b	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓
1c	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓
2a	-	-	-	✓	-	-	-	-	-	-	-	-
2a.1	✓	✓	-	✓	-	✓	-	-	-	-	-	-
2a.2	✓	✓	-	✓	-	-	-	✓	-	-	-	-
2a.3	✓	✓	-	✓	-	-	-	-	-	✓	-	-
3a	✓	✓	-	✓	-	-	-	-	-	-	-	-
3a.1	✓	✓	-	✓	-	-	-	-	-	-	-	-
3a.2	✓	✓	✓	✓	-	✓	✓	-	✓	✓	✓	-
3b	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	-	✓
3b.1	✓	✓	✓	✓	-	✓	✓	-	✓	✓	✓	-
3c	✓	✓	-	✓	-	-	-	-	-	-	-	-
3c.1	✓	✓	✓	✓	-	✓	✓	-	✓	✓	✓	-
3d	✓	✓	-	✓	-	-	-	✓	-	-	✓	-
3d.1	✓	✓	✓	✓	-	✓	✓	-	✓	✓	✓	-
4a	✓	✓	✓	✓	-	-	-	-	✓	-	-	-
4b	✓	✓	-	✓	-	-	-	✓	-	-	✓	-
4b.1	✓	✓	-	✓	✓	✓	✓	✓	✓	✓	✓	✓
5a	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓
5b	✓	✓	✓	✓	-	✓	-	-	-	-	-	-
5b.1	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	-	✓
5b.2	✓	✓	✓	✓	-	✓	-	-	-	-	-	-
5b.3	✓	✓	✓	✓	-	✓	✓	-	✓	✓	✓	-
5b.4	✓	✓	✓	✓	-	✓	-	-	-	-	-	-
5b.5	✓	✓	✓	✓	-	✓	-	-	-	-	-	-
5c	✓	✓	-	✓	-	✓	-	-	-	-	-	-
5c.1	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓
5c.2	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓
5c.3	✓	✓	-	✓	-	-	-	-	-	-	-	-
5d	✓	✓	-	✓	-	-	-	-	-	-	-	-
5d.1	✓	✓	-	✓	✓	-	-	✓	✓	✓	-	-
5d.2	✓	✓	✓	✓	-	✓	✓	-	✓	✓	✓	-
5d.3	✓	✓	-	✓	-	-	-	-	-	-	✓	-
6a	✓	✓	-	✓	-	✓	-	✓	-	✓	-	-
6a.1	✓	✓	-	✓	-	✓	-	✓	-	✓	-	-
6a.2	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-
6a.3	✓	✓	-	✓	✓	✓	-	✓	-	✓	-	-
6b	✓	✓	-	✓	-	✓	-	-	-	✓	-	-
6b.1	✓	✓	-	✓	-	✓	-	-	-	✓	✓	-
6c	✓	✓	-	✓	✓	✓	-	-	-	✓	-	-
6d	✓	✓	-	✓	-	✓	-	-	-	✓	-	-
6d.1	✓	✓	-	✓	-	✓	-	-	-	✓	-	-
6d.2	✓	✓	-	✓	✓	✓	-	-	-	✓	-	-
6d.3	✓	✓	-	✓	✓	✓	-	-	-	✓	-	-
6e	✓	✓	-	✓	✓	✓	-	-	-	✓	-	-
7a	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓
7a.1	✓	✓	-	✓	-	-	✓	-	✓	-	✓	✓
7b	✓	✓	-	✓	-	✓	✓	✓	✓	-	-	✓
7b.1	✓	✓	-	✓	-	✓	✓	✓	✓	-	✓	✓
7c	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	-	✓
7c.1	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓
7c.2	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓
7c.3	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓
7d	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓
7d.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8a	-	-	-	✓	-	-	-	-	-	-	-	-
8a.1	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	-	✓
8a.2	✓	✓	-	✓	✓	-	-	-	-	-	-	-
8b	✓	✓	-	✓	-	-	✓	✓	✓	✓	-	-
8b.1	✓	✓	-	✓	-	-	✓	-	✓	✓	-	✓
Total= 61	60	60	23	61	12	38	29	23	28	34	21	21

AIA	GDPR	EDPB	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK
1a	✓	✓	✓	✓	✓	✓	✓	✓	-	-	✓	✓
1b	✓	✓	✓	✓	✓	✓	✓	✓	-	-	✓	✓
1c	✓	✓	✓	✓	✓	✓	✓	✓	-	-	✓	✓
2a	-	-	-	-	-	-	-	-	-	-	-	-
2a.1	✓	✓	-	-	-	-	✓	-	✓	-	-	-
2a.2	✓	✓	-	-	-	-	-	-	-	-	-	-
2a.3	✓	✓	-	-	-	-	-	-	✓	-	-	✓
3a	✓	✓	✓	-	-	-	✓	-	-	-	-	-
3a.1	✓	✓	✓	-	-	-	✓	-	-	-	-	-
3a.2	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	✓
3b	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-	✓
3b.1	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	✓
3c	✓	✓	✓	-	-	-	✓	-	-	-	-	-
3c.1	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	✓
3d	✓	✓	✓	-	✓	✓	-	-	-	-	-	-
3d.1	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	✓
4a	✓	✓	-	-	-	-	-	-	-	-	-	-
4b	✓	✓	✓	-	✓	-	-	-	-	-	-	-
4b.1	✓	✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓
5a	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-	✓
5b	✓	✓	-	-	✓	-	-	-	-	-	✓	✓
5b.1	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓	✓
5b.2	✓	✓	-	-	✓	-	✓	-	-	-	✓	✓
5b.3	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	✓
5b.4	✓	✓	-	-	✓	-	✓	-	-	-	✓	✓
5b.5	✓	✓	-	-	✓	-	-	-	-	-	✓	✓
5c	✓	✓	-	-	-	-	✓	-	-	-	-	-
5c.1	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓
5c.2	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-	✓
5c.3	✓	✓	-	-	✓	-	✓	-	-	-	-	-
5d	✓	✓	-	-	-	-	-	-	-	-	-	-
5d.1	✓	✓	✓	-	-	✓	✓	-	-	✓	✓	-
5d.2	✓	✓	✓	✓	-	✓	-	✓	✓	✓	✓	✓
5d.3	✓	✓	-	-	✓	-	✓	-	-	-	-	-
6a	✓	✓	-	-	✓	✓	✓	-	-	-	-	-
6a.1	✓	✓	-	-	✓	✓	✓	-	-	-	-	-
6a.2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6a.3	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	-
6b	✓	✓	-	-	✓	-	-	-	-	-	-	-
6b.1	✓	✓	-	-	✓	-	✓	-	-	-	-	-
6c	✓	✓	✓	✓	✓	-	✓	-	✓	-	✓	-
6d	✓	✓	-	-	✓	-	-	-	-	-	-	-
6d.1	✓	✓	-	-	✓	-	-	-	-	-	-	-
6d.2	✓	✓	✓	✓	✓	-	✓	-	✓	-	✓	-
6d.3	✓	✓	✓	✓	✓	-	✓	-	✓	-	✓	-
6e	✓	✓	✓	✓	✓	-	✓	-	✓	-	✓	-
7a	✓	✓	✓	✓	-	-	-	-	-	✓	✓	-
7a.1	✓	✓	✓	✓	✓	-	✓	-	-	✓	✓	-
7b	✓	✓	✓	✓	✓	✓	✓	-	-	✓	✓	-
7b.1	✓	✓	✓	✓	✓	✓	✓	-	-	✓	✓	-
7c	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓
7c.1	✓	✓	✓	✓	-	-	-	-	-	✓	✓	-
7c.2	✓	✓	✓	✓	-	-	-	-	-	✓	✓	-
7c.3	✓	✓	✓	✓	-	-	-	-	-	✓	✓	-
7d	✓	✓	✓	✓	-	-	-	-	-	✓	✓	-
7d.1	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓
8a	-	-	-	-	-	-	-	-	-	-	-	-
8a.1	✓	✓	✓	-	-	✓	✓	✓	-	✓	-	✓
8a.2	✓	✓	✓	✓	✓	-	✓	-	✓	-	✓	-
8b	✓	✓	✓	-	✓	✓	✓	-	-	-	-	-
8b.1	✓	✓	✓	-	✓	-	✓	-	✓	-	-	-
Total= 61	60	60	41	28	40	27	37	18	22	25	34	24

References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[2] European Union. Regulation—EU—2024/1689—EN—EUR-Lex. EU AI Act.
URL https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[3] E. Drouard, O. Kurochkina, R. Schlich, D. Ozturk, The Interplay between the AI Act and the GDPR: 1 (2) 164–176. doi:10.21552/aire/2024/2/4.

[4] A. Thomaidou, K. Limniotis, Navigating Through Human Rights in AI: Exploring the Interplay Between GDPR and Fundamental Rights Impact Assessment 5 (1) 7. doi:10.3390/jcp5010007.
URL https://www.mdpi.com/2624-800X/5/1/7

[5] M. Grafenstein, Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR)doi:10.2139/ssrn.4104502.

[6] M. Draghi, The future of European competitiveness: Report by Mario Draghi.
URL https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en

[7] K. Demetzou, GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved, in: E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, S. Krenn (Eds.), Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data, Vol. 547, Springer International Publishing, pp. 137–154. doi:10.1007/978-3-030-16744-8_10.

[8] J. Schuett, Risk Management in the Artificial Intelligence Act 1–19doi:10.1017/err.2023.1.

[9] S. Barezzani, Data Protection Impact Assessment (DPIA), in: S. Jajodia, P. Samarati, M. Yung (Eds.), Encyclopedia of Cryptography, Security and Privacy, Springer Berlin Heidelberg, pp. 1–3. doi:10.1007/978-3-642-27739-9_1813-1.

[10] European Data Protection Board, EDPB guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01).
URL https://ec.europa.eu/newsroom/article29/items/611236

[11] P. Ryan, R. Brennan, H. J. Pandit, DPCat: Specification for an Interoperable and Machine-Readable Data Processing Catalogue Based on GDPR 13 (5) 244. doi:10.3390/info13050244.

[12] Commission nationale de l'informatique et des libertés, CNIL Privacy Impact Assessment.
URL https://www.cnil.fr/en/privacy-impact-assessment-pia

[13] ISO/IEC 29134:2023.
URL https://www.iso.org/standard/86012.html

[14] D. Golpayegani, H. J. Pandit, D. Lewis, To Be High-Risk, or Not To Be—Semantic Specifications and Implications of the AI Act's High-Risk AI Applications and Harmonised Standards, in: 2023 ACM Conference on Fairness, Accountability, and Transparency, ACM, pp. 905–915. doi:10.1145/3593013.3594050.

[15] H. J. Pandit, A Semantic Specification for Data Protection Impact Assessments (DPIA)doi:10.5281/ZENODO.6783203.

[16] A. Mantelero, The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template 54 106020. doi:10.1016/j.clsr.2024.106020.

[17] A. Calvi, D. Kotzinos, Enhancing AI fairness through impact assessment in the European Union: A legal and computer science perspective, in: 2023 ACM Conference on Fairness, Accountability, and Transparency, ACM, pp. 1229–1245. doi:10.1145/3593013.3594076.

[18] Commission Nationale de l'Informatique et des Libertes, CNIL AI how to sheets.
URL https://www.cnil.fr/en/ai-how-sheets

[19] J. Gerards, M. T. Schaefer, A. Vankan, I. Muis, Fundamental Rights and Algorithms Impact Assessment. 1–99.

[20] Datenschutzbehörde, Austria DPIA guide.
URL https://www.dsb.gv.at/download-links/dokumente.html

[21] Autorite de protection des Donnees, Belgium dpia guide.
URL https://www.autoriteprotectiondonnees.be/publications/decision-n-01-2019-du-16-janvier-2019.pdf

[22] Commission for Personal Data Protection, Bulgaria DPIA guide.
URL https://cpdp.bg/en/list-of-processing-operations-requiring-data-protection-impact-assessment-dpia-pursuant

[23] Digital Services Factory, Cyprus DPIA guide.
URL https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/ED786DE02E8020FCC225826000377143/$file/Indicative%20DPIA%20list.pdf

[24] Údajů Úřad, Czech DPIA guide.
URL https://uoou.gov.cz/profesional/metodiky-a-doporuceni-pro-spravce/posouzeni-vlivu-na-ochranu-osobnich-udaju

[25] Dataschutzkonferenz, German DPIA guide.
URL https://datenschutzkonferenz-online.de/media/ah/20181017_ah_DPIA_list_1_1_Germany_EN.pdf
[26] Datatilsynet, Denmark DPIA guide.
URL https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed/konsekvensanalyse/konsekvensanalyser
[27] Andmekaitse Inspektsioon, Estonia DPIA guide.
URL https://www.aki.ee/en/guidelines-legislation/cross-border-data-protection-impact-assessment
[28] Agencia Española de Protección de Datos, Spain DPIA guide.
URL https://www.aepd.es/documento/listas-dpia-en-35-4.pdf
[29] Tietosuoja Virasto, Finland DPIA guide.
URL https://tietosuoja.fi/vaikutustenarviointi
[30] Commission Nationale Informatique Libertes, France DPIA guide.
URL https://www.cnil.fr/sites/cnil/files/atoms/files/liste-traitements-aipd-requise.pdf
[31] Hellenic Data Protection Authority, Greece DPIA guide.
URL https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_gr/page2c_gr?opendocument
[32] Agencija za Podataka, Croatia DPIA guide.
URL https://azop.hr/procjena-ucinka/
[33] Nemzeti Adatvédelmi és Információszabadság Hatóság, Hungary DPIA guide.
URL https://naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list
[34] Data Protection Commission, Ireland DPIA guide.
URL https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments?utm_source=chatgpt.com#identifying-whether-a-dpia-is-required
[35] Persónuvernd, Iceland DPIA guide.
URL https://www.personuvernd.is/media/leidbeiningar-personuverndar/MAP-Mat-a-Ahrifum-a-Personuvernd.pdf
[36] Garante per la protezione dei dati personali, Italian dpia guide.
URL https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-
[37] Datenschutzstelle Liechtenstein, Liechtenstein DPIA guide.
URL https://www.datenschutzstelle.li/application/files/7615/9670/5293/DPIA_list_Liechtenstein_EN.pdf
[38] Valstybinė Duomenų Apsaugos Inspekcija, Lithuania DPIA guide.
URL https://vdai.lrv.lt/en/news/list-of-data-processing-operations-subject-to-the-requirement-to-perform-data-
[39] Commission nationale pour la protection des données, Luxembourg DPIA guide.
URL https://cnpd.public.lu/en/professionnels/obligations/AIPD/liste-dpia.html
[40] Datu valsts inspekcija, Latvia DPIA guide.
URL https://www.dvi.gov.lv/lv/novertejums-par-ietekmi-uz-datu-aizsardzibu-nida
[41] Information and Data Protection Commissioner, Malta DPIA guide.
URL https://idpc.org.mt/for-organisations/data-protection-impact-assessment/
[42] Autoriteit Persoonsgegevens, Netherlands DPIA guide.
URL https://autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668
[43] Datatilsynet, Norweigan DPIA guide.
URL https://www.datatilsynet.no/en/#:~:text=Do%20you%20wonder%20if%20you,always%20will%20require%20a%20DPIA.
[44] Urząd Ochrony Danych Osobowych, Poland DPIA guide.
URL https://archiwum.uodo.gov.pl/pl/424
[45] Comissão Nacional deProtecção de Dados, Portugal DPIA guide.
URL https://www.cnpd.pt/organizacoes/obrigacoes/avaliacao-de-impacto/
[46] Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Romania DPIA guide.
URL https://www.dataprotection.ro/servlet/ViewDocument?id=1870
[47] Integritetsskyddsmyndigheten, Sweden DPIA guide.
URL https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/
[48] Úrad na ochranu osobných údajov Slovenskej republiky, Slovakia DPIA guide.
URL https://dataprotection.gov.sk/en/legislation-guidelines/guidelines-faq/office-guidelines/list-processing-operations-that-are-subject-an-impact-assessment/

[49] Informacijski Pooblascenec, Slovenia DPIA Guide.
URL https://www.iprs.si/dokumenti/razno/Seznam_dejanj_obdelav_osebnih_podatkov__za_katere_velja_zahteva_po_izvedbi_ocene_ucinka_v_zvezi_z_varstvom_osebnih_podatkov.pdf
[50] European Commission, eTranslation.
URL https://commission.europa.eu/resources-partners/etranslation_en
[51] European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD).
[52] J. Naves, P. Rijcken, EU model contractual AI clauses to pilot in procurements of AI.
[53] M. Castelli, L. C. Moreau, Ph.D., The Cycle of Trust and Responsibility in Outsourced AI, in: Proceedings of the 2nd Workshop on Trustworthy Natural Language Processing (TrustNLP 2022), Association for Computational Linguistics, pp. 43–48. doi:10.18653/v1/2022.trustnlp-1.4.
[54] A. Mantelero, The Ai Act's Fundamental Rights Impact Assessment. doi:10.2139/ssrn.4782126.
[55] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, J. Flake, Data Privacy Vocabulary (DPV) – Version 2 (Apr. 2024). arXiv:2404.13426.
[56] T. Rintamaki, H. J. Pandit, Developing an Ontology for AI Act Fundamental Rights Impact Assessments. doi:10.48550/ARXIV.2501.10391.
URL https://arxiv.org/abs/2501.10391
[57] T. Rintamaki, H. J. Pandit, Towards An Automated AI Act FRIA Tool That Can Reuse GDPR's DPIA. doi:10.48550/ARXIV.2501.14756.
URL https://arxiv.org/abs/2501.14756