

Pride & *Prejudice*

Data Protection, AI and the Art of Assessing into Compliance

Cool workshop // March 7th, 2024 // Tea Mustać, Peter Hense



Peter Hense



Tea Mustać



Search

Sign in

Home

Shorts

Subscriptions

You

History

Sign in to like videos, comment, and subscribe.

Sign in

Explore

Trending

Music

Movies & TV

Live

Gaming

News



RegInt - DECODING AI REGULATION

Evil Legal

11 videos 106 views Last updated on Feb 27, 2024

Play all

Shuffle

When you are stuck in a current - don't fight it; get to the bottom and swim to the other side. Same with AI - to help you get to the bottom and swim across we've crafted a series of episodes - think of them as your AI GPS, providing direction, structure, and a bird's-eye view on all things AI.

1



RegInt: Decoding AI Regulation #11 | The Copyright Crusade

Evil Legal • 44 views • Streamed 8 days ago

2



RegInt: Decoding AI Regulation #10 | Caught Between Sci-Fi and Common Sense

Evil Legal • 48 views • Streamed 1 month ago

3



RegInt - Decoding AI Regulation #9 | New Year's AI Resolution

Evil Legal • 55 views • Streamed 2 months ago

4



RegInt - Decoding AI Regulation #8 | AI Act trilogue - from hero to zero

Evil Legal • 42 views • Streamed 3 months ago

5



RegInt: Decoding AI Regulation | News Signals - AI Revelations Reviewed

Evil Legal • 44 views • Streamed 4 months ago

6



RegInt: Decoding AI Regulation #6 | Unmasking AI - Faces Behind the Code

Evil Legal • 120 views • Streamed 5 months ago

150 +

DPO appointments in 2024

60 +

Collective actions since 2017

400 +

DPA Proceedings since 2012

500 +

Individual lawsuits since 2012

60 +

DPIAs since 2018

Hot topics 2024

***Is AI on a collision course
with GDPR?***

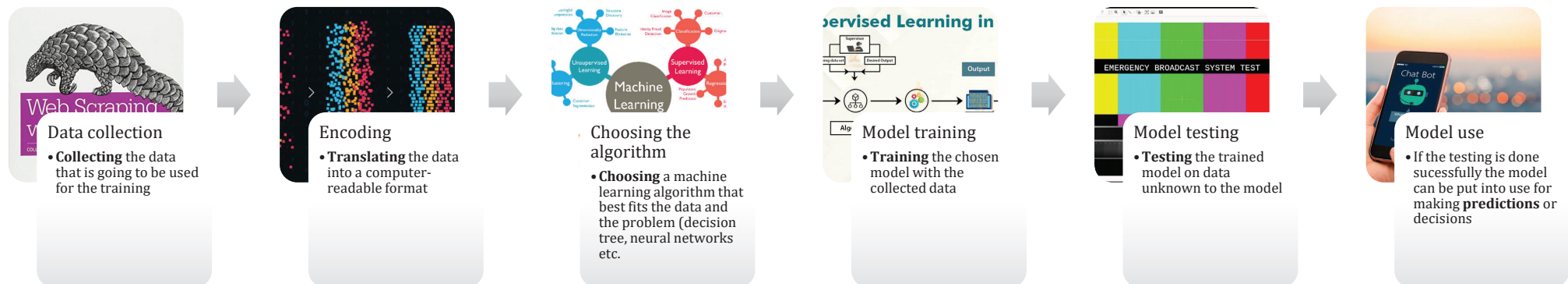


AI System as defined by the AI Act, Art. 3.1

(1) 'AI system' is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;



Machine Learning (ML), Step by Step



GDPR Kryptonite for training data

- **Scraping Special Category Data (SCD) requires explicit consent***
 - Any data that may reveal sensitive information is considered SCD
 - No intention to process SCD is required; Controller required to check first, process later
 - Web scraping severely limited (“manifestly made public”)
 - “Legitimate interest”: No children’s data, No commercial surveillance, no copyright violations
- **Violating GDPR is costly****
 - “Loss of control” over personal data constitutes immaterial damage
- **EU “class actions” incoming*****
 - The Collective Redress Directive empowers consumers to unite and initiate lawsuits, seeking both model deletion and compensation (unjust enrichment and damages)
 - Reversed burden of proof confirmed in almost every CJEU decision in 2023

*C-184/20 – Etikos Komisija and C-252/21 – BKartA v. Meta, **C-456/22 – Ummendorf; ***Directive (EU) 2020/1828

GDPR Kryptonite for AI systems

- **Any decision that creates “legal” or “similarly significant effects” is subject to the prohibition (!) in Art. 22.1 GDPR**
 - CJEU is the “Guardian” of the Charter of Fundamental Rights and interprets secondary law accordingly
 - What a “decision” is, remains unclear, but the CJEU shifted responsibility to a very early stage of data processing: The creation of values on which downstream decisions “draw strongly” or for which the created value “plays a determining role”.
 - “Establishment of a probability value based on personal data relating to a person and concerning that person’s ability to repay a loan in the future”
 - Additional safeguards (more than just Art. 22.3 GDPR) according to the **risk analysis**, considering discriminatory effects

(Some of) **The Intersections**



Facial recognition



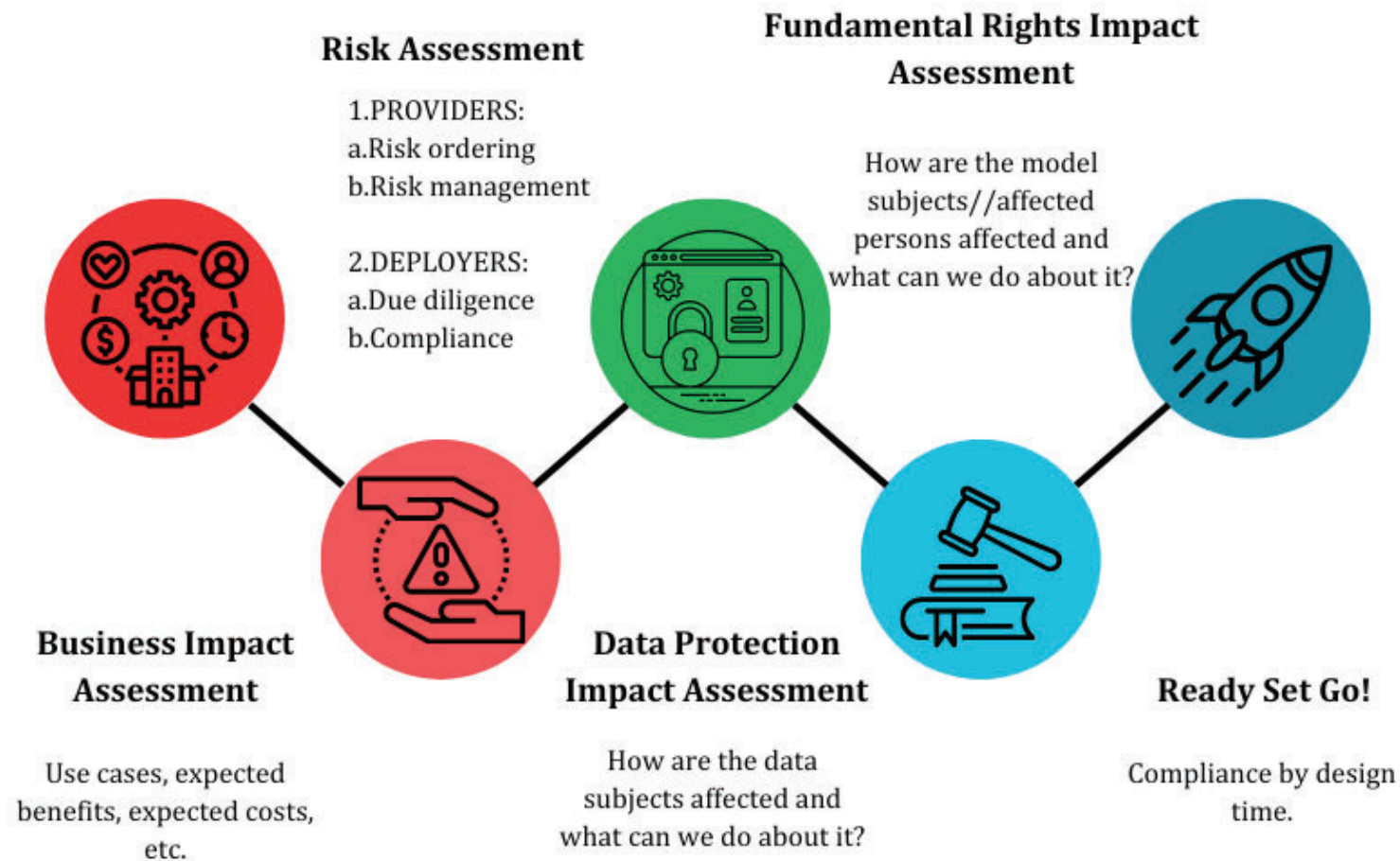
Credit scoring



Large language models



AI Impact Assessment(s) Project Initialization



Spot the Difference: FRIA, AI Risk Assessment and DPIA

The ,Who‘

DPIA

- (7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

AI Risk Assessment

- (2) ‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or a general purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge;

FRIA

- (4) ‘deployer means any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;

Spot the Difference: FRIA, AI Risk Assessment and DPIA

The ,When‘

DPIA

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
 - (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
 - (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
 - (c) a systematic monitoring of a publicly accessible area on a large scale.

AI Risk Assessment

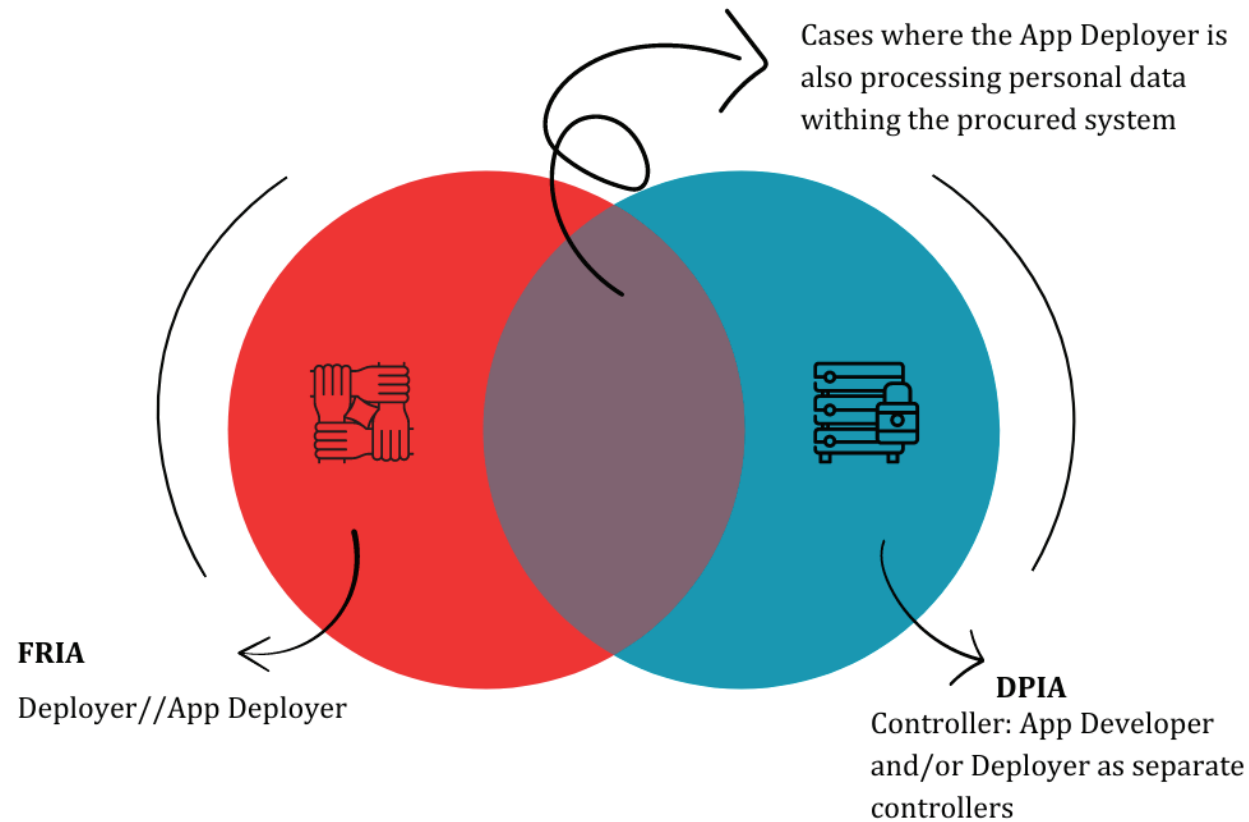
A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

FRIA

Prior to deploying a high-risk AI system as defined in Article 6(2), with the exception of AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law or private operators providing public services and operators deploying high-risk systems referred to in Annex III, point 5, (b) and (ca) shall perform an assessment of the impact on fundamental rights that the use of the system may produce. For that purpose, deployers shall perform an assessment consisting of:

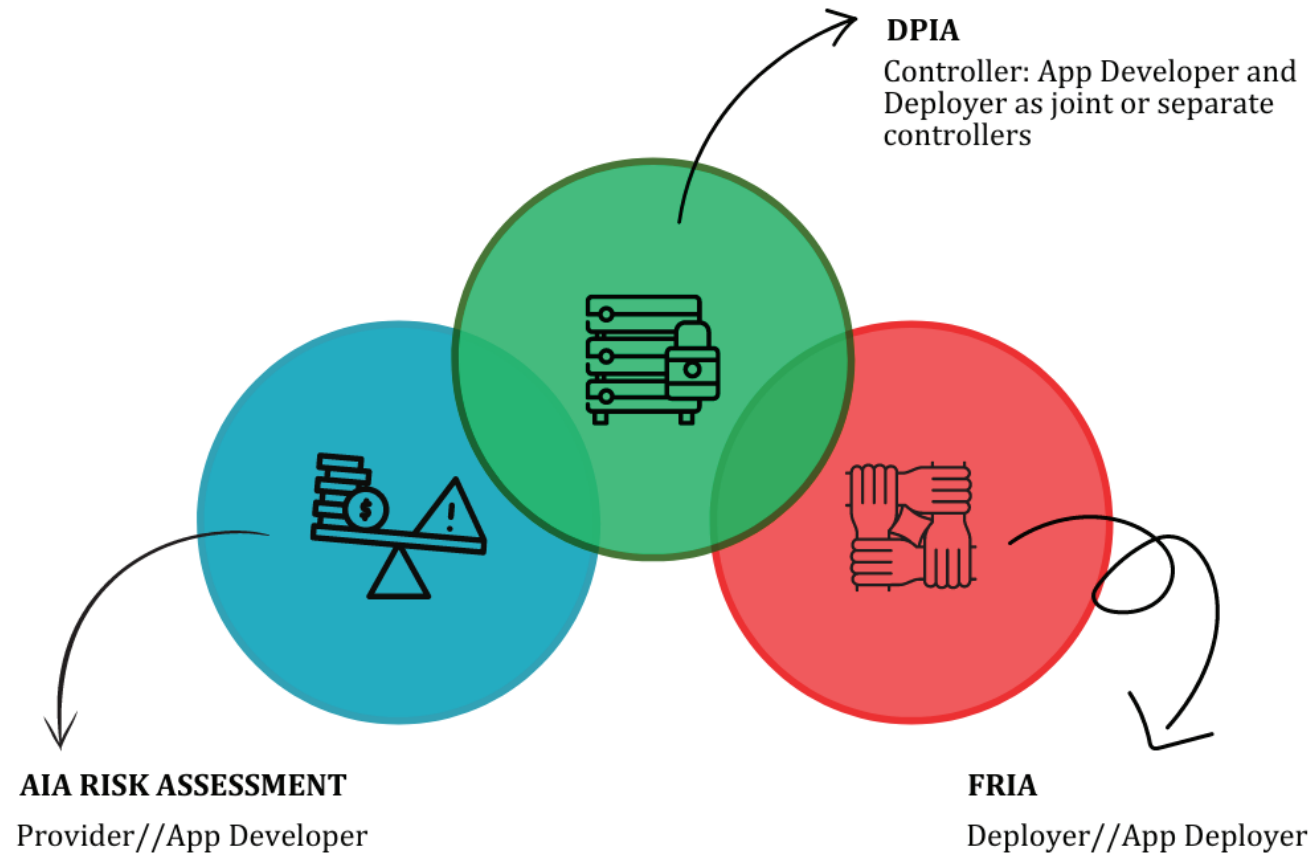
Spot the Difference: FRIA, AI Risk Assessment and DPIA

The Time to get Practical: App Procurement



Spot the Difference: FRIA, AI Risk Assessment and DPIA

The Time to get Practical: App Commissioning



App-commissioning and (joint)controllership

C-683/21 Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija

On controllership:

“an entity which has entrusted an undertaking with the development of a mobile IT application and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application may be regarded as a controller...

even if that entity has not itself performed any processing operations in respect of such data, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application

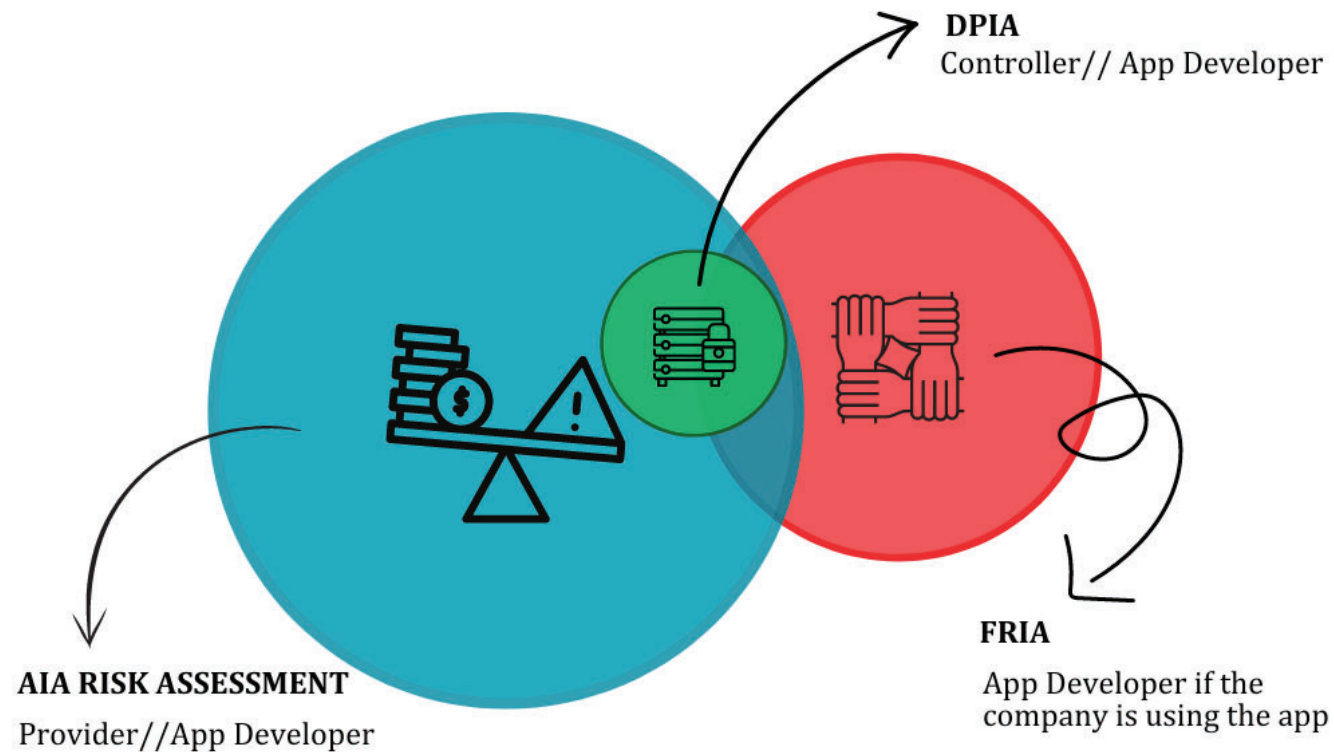
unless... that entity expressly objected to such making available and to the resulting processing of personal data.”

On joint-controllership:

the classification of two entities as joint controllers does not require that there be an arrangement between those entities ...

Spot the Difference: FRIA, AI Risk Assessment and DPIA

The Time to get Practical: App Development



Spot the Difference: FRIA, AI Risk Assessment and DPIA

The ,What‘

DPIA

- (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

AI Risk Assessment

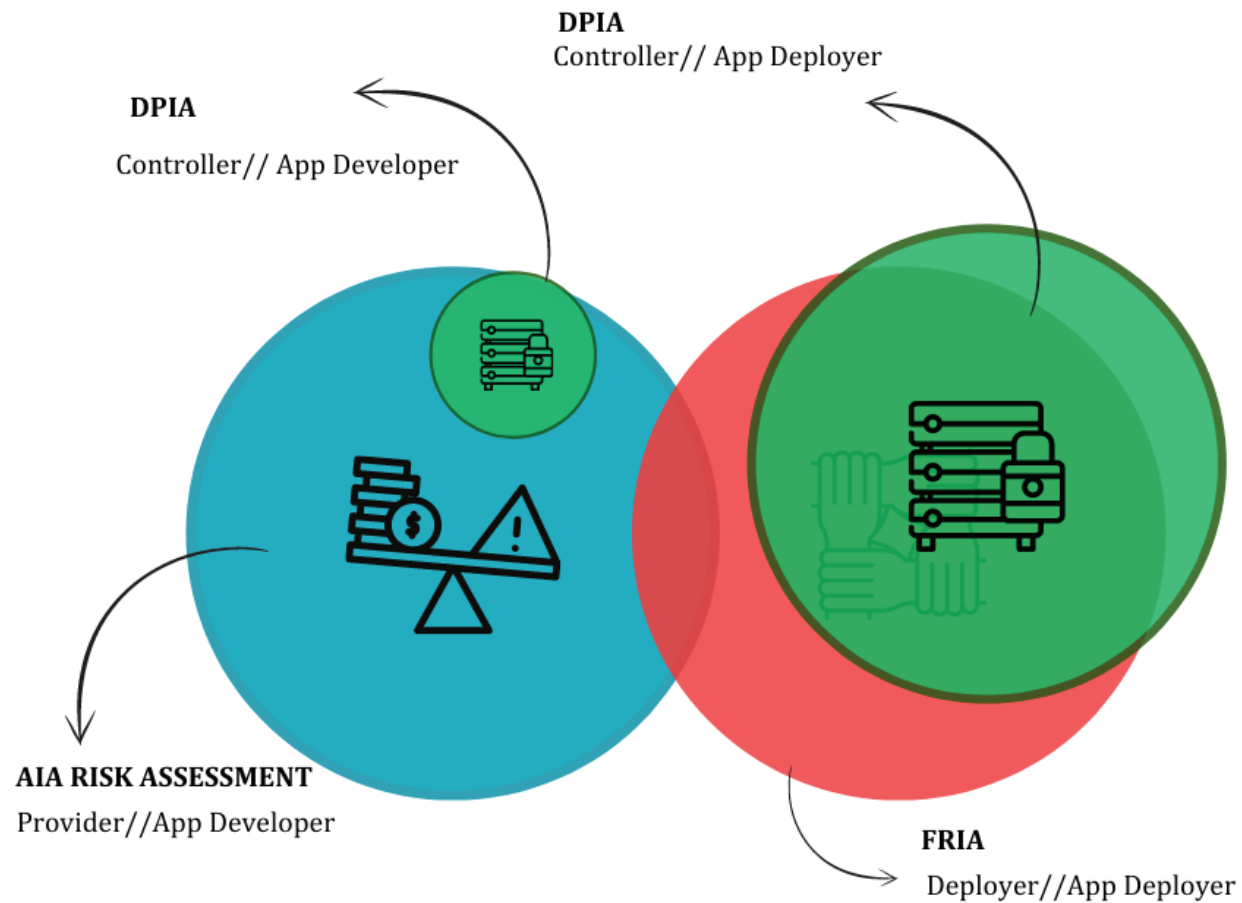
- (a) identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to the health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;
- (b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;
- (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;
- (d) adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point a of this paragraph in accordance with the provisions of the following paragraphs.

FRIA

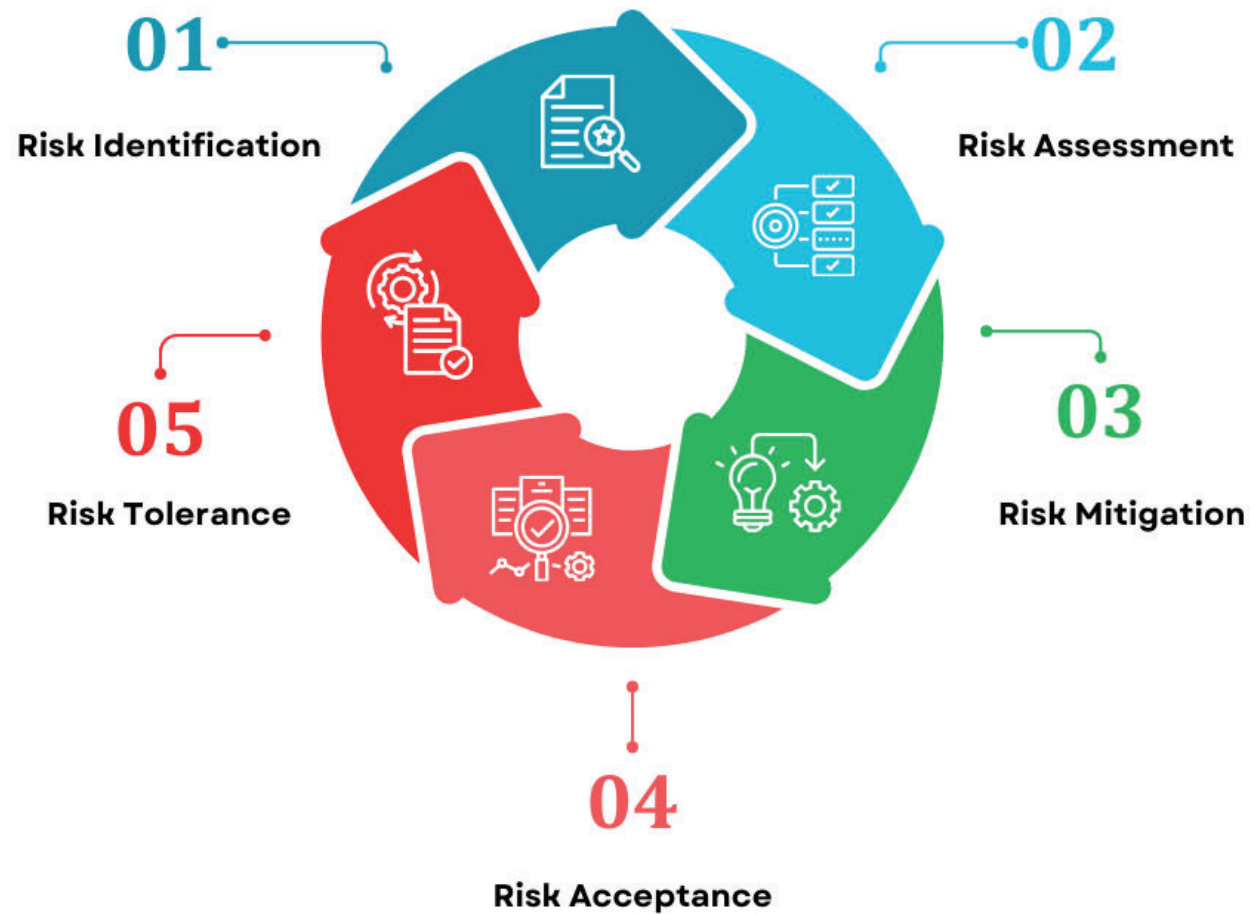
- (a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;
- (b) a description of the period of time and frequency in which each high-risk AI system is intended to be used;
- (c) the categories of natural persons and groups likely to be affected by its use in the specific context;
- (d) the specific risks of harm likely to impact the categories of persons or group of persons identified pursuant point (c), taking into account the information given by the provider pursuant to Article 13;
- (e) a description of the implementation of human oversight measures, according to the instructions of use;
- (f) the measures to be taken in case of the materialization of these risks, including their arrangements for internal governance and complaint mechanisms.

Spot the Difference: FRIA, AI Risk Assessment and DPIA

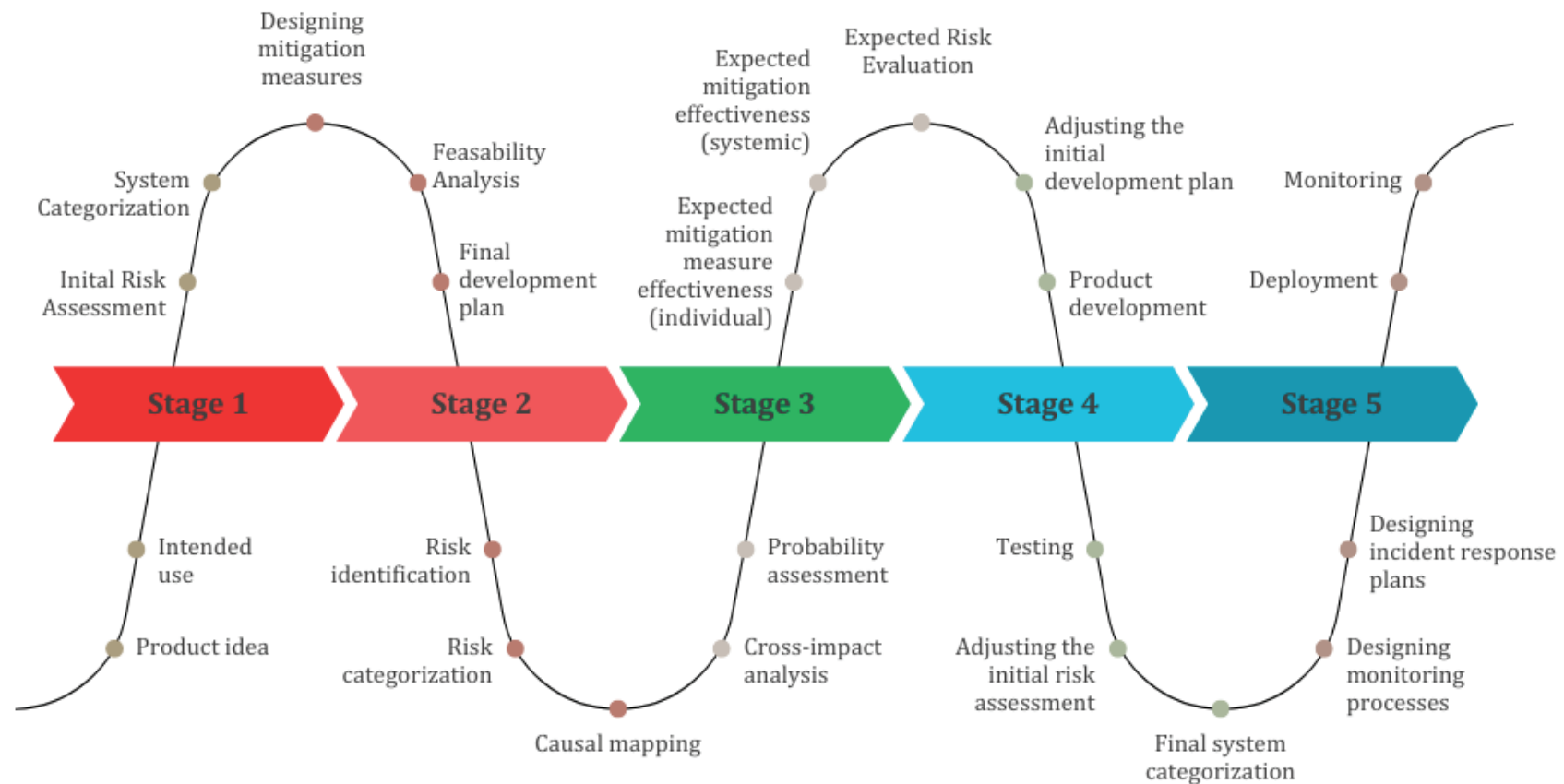
The Time to get Practical: Assessments contents and overlaps



It's all about
Risk Management



AI Risk Assessment Cycle



Contact

Peter Hense

peter.hense@spiritlegal.com

Tea Mustać

Tea.mustac@spiritlegal.com

www.spiritlegal.com
