



Alpine Privacy Days

Zuoz

7th & 8th of March 2024

AI & Privacy Concerns – the view of the authority

Michael Will





Scope, Art. 2 Abs 5a AIA:

Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect Regulations (EU) 2016/679 and (EU) 2018/1725 and Directives 2002/58/EC and (EU) 2016/680, **without prejudice to arrangements provided for in Article 10(5) and Article 54 of this Regulation**



Legal basis to fight bias, Art. 10 Abs. 5 AIA

- ✓ legal basis corresponding Art. 9 DS-GVO
- ✓ clear limitations

To the extent that it is strictly necessary for the purposes of ensuring bias detection and correction in relation to the high-risk AI systems (...) the providers of such systems may exceptionally process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, (...) subject to appropriate safeguards for the fundamental rights and freedoms of natural persons.

In addition to provisions set out in the Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725, all the following conditions shall apply in order for such processing to occur:

- (a) the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;
- (b) the special categories of personal data processed for the purpose of this paragraph are subject to technical limitations on the re-use of the personal data and state of the art security and privacy-preserving measures, including pseudonymisation;
- (c) the special categories of personal data processed for the purpose of this paragraph are subject to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure only authorised persons have access to those personal data with appropriate confidentiality obligations;
- (d) the special categories of personal data processed for the purpose of this paragraph are not to be transmitted, transferred or otherwise accessed by other parties;
- (e) the special categories of personal data processed for the purpose of this paragraph are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whatever comes first; (....)

6. For the development of high-risk AI systems not using techniques involving the training of models, paragraphs 2 to 5 shall apply only to the testing data sets.



“Sandbox”-privilege, Art. 54 AIA

- ✓ allows further processing
- ✓ clear limitations
- ? legal basis

Article 54 Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox

1. In the AI regulatory sandbox personal data lawfully collected for other purposes may be processed solely for the purposes of developing, training and testing certain AI systems in the sandbox when all of the following conditions are met:
- (a) AI systems shall be developed for safeguarding substantial public interest by a public authority or another natural or legal person governed by public law or by private law and in one or more of the following areas: (...)
 - (b) the data processed are necessary for complying with one or more of the requirements referred to in Title III, Chapter 2 where those requirements cannot be effectively fulfilled by processing anonymised, synthetic or other non-personal data; (c) there are effective monitoring mechanisms to identify if any high risks to the rights and freedoms of the data subjects, as referred to in Article 35 of Regulation (EU) 2016/679 and in Article 39 of Regulation (EU) 2018/1725, may arise during the sandbox experimentation as well as response mechanism to promptly mitigate those risks and, where necessary, stop the processing;
 - (d) any personal data to be processed in the context of the sandbox are in a functionally separate, isolated and protected data processing environment under the control of the prospective provider and only authorised persons have access to that those data; (e) providers can only further share the originally collected data in compliance with EU data protection law. Any personal data created in the sandbox cannot be shared outside the sandbox; (...)



Privacy and accountability – really topics of the AIA?

The concept of presumption of conformity

- ✓ typical product law
- ✓ some conditions
- ? scope, binding for whom ?

Art. 48 AIA

EU declaration of conformity

1. The provider shall draw up a written machine readable, physical or electronically signed EU declaration of conformity for each high-risk AI system and keep it at the disposal of the national competent authorities for 10 years after the AI high-risk system has been placed on the market or put into service. The EU declaration of conformity shall identify the high-risk AI system for which it has been drawn up. (...).
2. The EU declaration of conformity shall state that the high-risk AI system in question meets the requirements set out in Chapter 2 of this Title. The EU declaration of conformity shall contain the information set out in Annex V and shall be translated into a language that can be easily understood by the national competent authorities of the Member State(s) in which the high-risk AI system is placed on the market or made available.
3. (...)
4. By drawing up the EU declaration of conformity, the provider shall assume responsibility for compliance with the requirements set out in Chapter 2 of this Title. The provider shall keep the EU declaration of conformity up-to-date as appropriate



AI related Privacy Concerns Authorities' Perspectives



Emerging Guidelines – some examples

- preliminary guidelines/discussion papers
- on national level, not yet by EDPB (mandated; not scope of the AI-Task Force)
- various additional support
- no designation of AI- competent authority on national level so far





AI related Privacy Concerns



Building Blocks

ROPA

Roles

Personal Data
?

Legal Basis

Security

DPIA

Transparency

Data subject's
rights

AI as a service



- not exhaustive

Checkliste

I. Konzeption des Einsatzes und Auswahl von KI-Anwendungen

1. Einsatzfelder und Zwecke bestimmt?
2. Einsatzfelder ohne personenbezogene Daten?
3. Datenschutzkonforme Trainingsdaten?
4. Einsatzfelder rechtmäßig?
5. Rechtsgrundlage für die Datenverarbeitung?
6. Keine automatisierte Letztentscheidung
7. Geschlossenes oder offenes System?
8. Transparenz
9. Transparenz und Wahlmöglichkeit hinsichtlich KI-Training
10. Transparenz und Wahlmöglichkeit hinsichtlich Eingabe-Historie
11. Berichtigung und Löschung
12. Datenschutzbeauftragte und Beschäftigtenvertretung einbinden

II. Implementierung von KI-Anwendungen

13. Verantwortlichkeit festlegen und verbindlich regeln
14. Interne Regelungen treffen
15. Datenschutzfolgenabschätzung
16. Beschäftigte schützen, betriebliche Accounts einrichten
17. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
18. Datensicherheit
19. Beschäftigte sensibilisieren

- AI with or without personal data
- clear concept/purpose - > Governance
- legal basis for data training -> next
- legal basis for personal data in prompts/other input
- scope of Art. 9 - [ECJ'S](#) „infection theory“

Rn. 89: In that context, it should be noted that the operations entailing the collection, the linking and the use of the data, referred to in Questions 3 to 5, may include both sensitive data within the meaning of Article 9(1) of the GDPR and non-sensitive data. It must be made clear that, where a set of data containing both sensitive data and non-sensitive data is subject to such operations and is, in particular, collected *en bloc* without it being possible to separate the data items from each other at the time of collection, the processing of that set of data must be regarded as being prohibited, within the meaning of Article 9(1) of the GDPR, if it contains at least one sensitive data item and none of the derogations in Article 9(2) of that regulation applies.



Race for Big Data – service provider as processor or controller ?





How to get a data lake - Service & AI providers' framework

- Customer data processed **within** the **scope of instruction** = provider acts as **processor**
 - Quality of service provisioning in a cloud service context changed over time as the serviced provided changed significantly – e.g. continuous improvement of already existing intelligent features
 - How granular must the instructions be?
- Customer data processed **outside of the scope** of instruction = provider acts as **controller**
 - Art. 28 (10) GDPR – GDPR infringement? (-)
- Contractual **authorization** from customer
 - Meaning of authorization?
 - Exclusion from scope of instruction (*Dispens*)
- How much information must be provided to the customer to enable an **informed decision**?
- Interplay between instruction and **purpose limitation**





Thank you for listening and discussing !

