Lawful AI Processing Logic Flow

ANONOS®

Anonymization

Can AI goals be achieved by processing anonymous data that is never relinkable to the identity of individuals?

YES → Consider processing AI using "Anonymous" data that is outside the jurisdiction of the GDPR under Recital 26 if the data cannot be used to reidentify individuals notwithstanding all of the means reasonably likely to be used by the controller or by another person, considering all objective factors, such as the costs of and the amount of time required for identification, available technology at the time of processing and technological developments since the time of data collection.

NO ↓

Consent

Is it possible to describe the AI processing at the time of data collection so that consent is freely given, specific, informed, and unambiguous, notwithstanding AI technologies' inherent complexity and unpredictability?

YES → Consider using Article 6(1)(a) Consent as the legal basis for AI processing, keeping in mind the requirements to: (i) provide an alternate means for the data subject to receive desired benefits without providing consent so that consent is "freely given"; (ii) notify the data subject of the controller's identity and the identity of third parties with whom the data will be shared and describe how it will be used and the purpose of the processing; (iii) once consent is secured to authorize specific processing, respect any subsequent withdrawal of consent (consent must be as easy to withdraw as it is to provide) and stop the processing authorized by consent; and (iv) not switch from the legal basis of consent to another legal basis if the data subject withdraws consent.

NO ↓

Contract

Is AI processing essential for the proper performance of the contract between the controller and the data subject, and is it true that there are no workable, less intrusive alternative means of processing?

YES → Consider using Article 6(1)(b) Necessary for Contract as the legal basis for AI processing, keeping in mind that: (i) If a less intrusive alternative means of processing exists, the processing is not 'necessary' to perform the contract; (ii) processing should only involve as much data as necessary to fulfill the purposes of the contract; collecting and processing excess data can lead to non-compliance; and (iii) If several services or elements of a service are bound together in one contract but they can reasonably be performed independently, each service or element needs to be assessed separately to determine what processing is objectively necessary to perform that service or element.

NO ↓

Legitimate Interests

Will the controller inform data subjects at the time of data collection of the legitimate interest being pursued by the data controller/third party and the technical controls being used to protect the data subjects' interests? Is the least identifiable data being processed using technical controls that ensure the processing is adequate, relevant, and limited to what is necessary? For example**,** Statutory Pseudonymization technical controls[1] limit relinking to identity only as authorized under controlled conditions. **Do the technical controls used to protect the data perform effectively at the actual scale of processing in order to avoid the interests of data subjects taking precedence over the legitimate interests of the controller or third party?**

YES → Consider using Article 6(1)(f) Legitimate Interest as the legal basis for AI processing, keeping in mind that the benefits of using Legitimate Interests as a legal basis under the GDPR include: (i) under Article 17(1)(c), if a data controller can show they "have overriding legitimate grounds for processing" supported by technical and organizational measures to satisfy the balancing of interest test, they have greater flexibility in complying with the Right to be Forgotten requests; (ii) under Article 18(1)(d), a data controller has flexibility in complying with requests to restrict the processing of personal data if they can show they have technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the privacy of the data subject is protected; (iii) under Article 20(1), data controllers using Legitimate Interests processing are not subject to the right of portability, which applies only to consent-based processing; and (iv) under Article 21(1), a data controller using Legitimate Interests processing may show they have adequate technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the rights of the data subjects are adequately protected. However, data subjects always have the right under Article 21(3) not to receive direct marketing outreach due to such processing.

NO ↓

[1] **Statutory Pseudonymization technical controls** enable controllably reversible de-identified data that is compliant with GDPR Article 4(5). See www.Pseudonymization.com

Unlawful Processing?

AI processing is likely unlawful under the GDPR unless the processing is necessary (i) for compliance with a legal obligation under EU law or the laws of a Member State - Article 6(1)(c), (ii) to protect the vital (life and death) interests of the data subject - Article 6(1)(d), or (iii) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller - Article 6(1)(e),

- Download this infographic at www.LegitimateInterestAnalytics.com

- Read the related article at https://iapp.org/news/a/beyond-gdpr-unauthorized-reidentification-and-the-mosaic-effect-in-the-eu-ai-act/