GDPR MODEL DRAFT

Towards a 21st-Century Regulatory Framework

Distinct Proposals to Amend the GDPR

Frank Ingenrieth, LL.M.

Independent Lawyer (Germany) | https://ingenrieth-online.de

DOI: 10.13140/RG.2.2.30130.77762

Purpose & Approach

The European Commission is addressing the need to amend the GDPR. Critics argue current updates are either excessive or purely cosmetic.

This Model Draft aims to:

- Go beyond determining needs by suggesting concrete drafted updates.
- Align GDPR provisions with 21st-century practical opportunities.
- Create a "single source of truth" for practitioners, academia, and legislators.

The Vision & Need for Reform

Beyond cosmetic updates: A conceptual rethink of European Data Protection architecture.

Determination of Needs

The Model Draft aims to move beyond mere academic determination of needs. It suggests drafted updates that align identification needs with 21st-century opportunities.

A One-Stop Reference: This document serves as a "One Source of Truth" for practitioners, academia, and legislators to critically reflect upon.

SECTION I

Core Definitions

Redefining Core Definitions

Shifting an open-end concept into a clearly distinct approach.

Individual Related Data (IRD)

A new concept replacing the traditional "Personal Data". It covers any information that is or can be referred to a **single Data Subject**.

Identifiers

Any means- piece or set of information - by which a Data Subject can be identified, including direct/indirect and static/dynamic means.

Identification Reimagined

Genuine vs. Non-Genuine

- **Genuine Identification:** Suffices to distinctively determine and potentially physically locate a Data Subject.

- **Non-Genuine Identification:** Information refers to a subject but doesn't suffice for distinctive determination.

Direct vs. Indirect Identifiers

Direct

Information by which the Data Subject can be directly identified without consultation of other sources.

Indirect

Requires additional information or consultation of other sources to bridge the gap to the Data Subject.

Identifiability

The inherent possibility to attribute information to a subject by means of Identification.

SECTION II

Articles 6 and 9 - Justification et al

Art. 6: Justified Processing

- **Justifications:** A revised framework clarifying the interplay between Art. 6 and Art. 9 GDPR.
- **Legitimate Interests:** Primary justification for processing that does not unduly harm fundamental rights.
- **Performance of Contract:** Necessary steps taken at the request of the data subject.
- **Public Interest:** Task performance carried out in the exercise of official authority.
- **Manifestly Public:** Processing data made public by the subject without technical objections.

The Role of Consent

EXCEPTIONAL CASE

Justification of Last Resort

Consent is relegated to **exceptional cases**. It only applies if no other justifications (legitimate interest, contract, etc.) apply.

Strict Barrier: Once processing is justified by consent, it cannot be alternatively justified by other legal bases if the consent fails.

Risk-Based Oversight

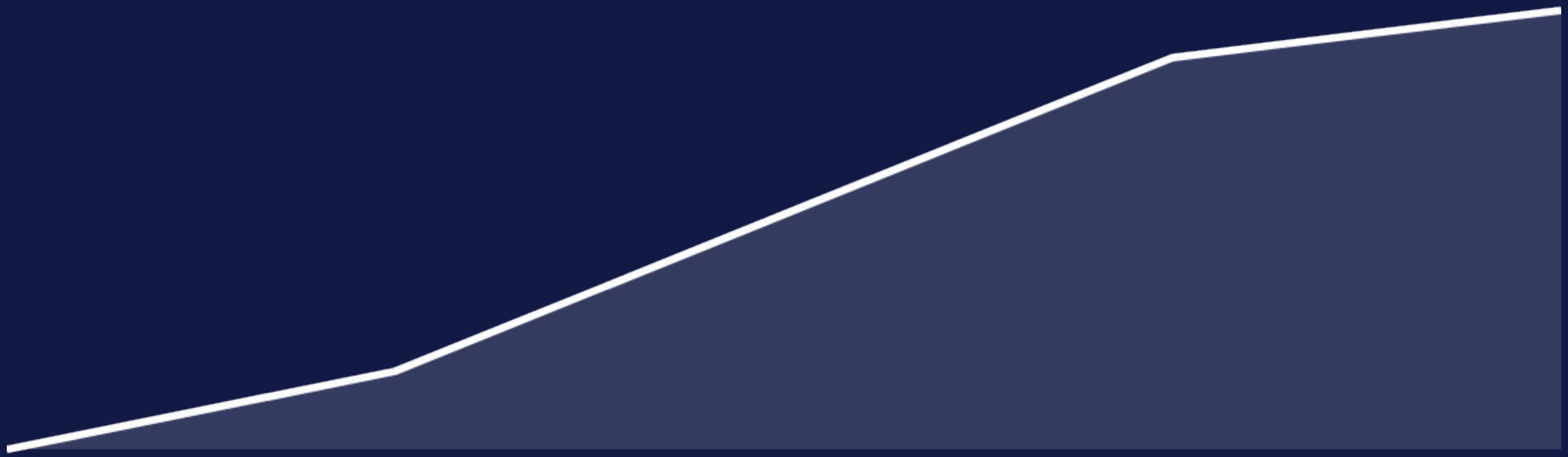
The Model Draft introduces rigorous management of high-risk identifiers:

- **Lists:** The European Commission maintains biennial lists of "High" and "Higher" risk IRD and identifiers.
- **Cryptographic Means:** High-risk identifiers must not be processed in the clear; they require adequate cryptographic protection.
- **Technical Measures:** IRD qualifying as "non-genuinely identified" is subject to strict technical and organisational measures.

High Risk Management

Category	Risk Factor	Regulator Requirement
High Risk IRD	Identity theft, financial fraud	Delegated Acts (evaluated biennially)
High Risk Identifiers	Cross-device tracking, biometrics	List maintained by Commission
Remote Processing	Cloud/Server side storage	Prohibited for High Risk unless allowed

Risk-Based Technical Safeguards



Standard IRD

Higher Risk

High Risk (Crytographic Needs)

The Model mandates that **High Risk Identifiers** must not be processed in the clear; they require adequate cryptographic means to prevent abuse and re-creation.

Refined Right to Object

Evidence-Based Objection

Limited to cases where processing causes **disproportionate harm** to fundamental rights.

For non-genuinely identified data, stakeholders and data subjects can object via supervisory authorities if processing is generally disproportionate.

- **Harm Threshold:** Limited to cases of disproportionate individual harm that cannot be reasonably mitigated.
- **General Disproportionality:** Stakeholders can object to non-genuinely identified data processing if it proves generally disproportionate.
- **Supervisory Review:** Claims of general disproportionality follow a structured review process by supervisory authorities.

Feedback & Contribution

The Model Draft is a living document.
Practitioners and academics are invited to critically reflect and comment.

DOI: 10.13140/RG.2.2.30130.77762

Frank Ingenrieth, LL.M.
https://ingenrieth-online.de