Data Security on the Ground:

Investigating Technical and Legal Requirements under the GDPR

Maria Konstantinou, Tina Marjanov, Magdalena Jozwiak, Dayana Spagnuelo

1. Problem

Article 32 of the General Data Protection Regulation - "Security of processing": *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."*

Research question: What are suitable measures to guarantee technical and legal compliance with GDPR Art. 32?

2. Methodology

Approach: Analyze court cases and fines to identify suitable measures, with steps:

1. Literature study (legal technical)
2. Create ontology of main case characteristics identified in literature study
3. Annotate cases* based on ontology
4. Analyze case characteristics

Case Descriptives: 20 cases across 13 EU+UK countries with total fines of more than 36,000,000 € (2,000 € - 27,800,000 €)

3. Ontology

Category	Possible values
GENERAL	
Decision, Country & DPA, Date, Fine, Other GDPR articles	
TECHNICAL	
Stage of processing	Collection/Storage/Processing/Destruction
Origin of threat	Internal/External
Maliciousness	Yes/No
Data type and format	Digital/Analog, Text, Pictures, Video
Mistake type	Human, Organizational, Technical
Requirements broken	Access control/Confidentiality/Integrity/Availability/Testing & audits
LEGAL	
Data breach	Yes/No
Type of data breach	Unauthorized access/Unlawful processing
GDPR infringement	Inherent risk in large datasets/Sensitive data
Cause of infringement	Inadequate implementation of security measure/Faulty code
LEGAL - RISK FACTORS	
Scope of processing	Increased data quantity/State organizations holding large datasets
Nature of data	Financial/Health/Educational
Kind of data subject	Students/Patients
Kind of data controller	State/Private organization, Large/Small
LEGAL - HARM	
Likelihood	Low/Medium/High
Severity	Low/Medium/High
Type of harm	Material: Identity theft/Financial loss Moral: Emotional distress/Chilling effect
Right/freedom affected	Privacy/Expression
LEGAL - TECHNICAL & ORGANIZATIONAL MEASURES	
Operational readiness	Staff training/ISO implementation
Remedies post factum	Swift notification/Operational remedies

4. Technical analysis

Depending on case properties (ontology values), we recognize 4 classes:

I. Coordinated high tech attack

- *What:* targeted hack, malware, cross-site scripting
- *Where:* bigger data controller, large datasets
- *Do:* implement highest industry standards (ISO/IEC), regular auditing and testing, dedicated IT/security staff

II. In breach of GDPR, but no incident

- *What:* insufficient access control, auditing, or protocols, too broad authorization
- *Where:* medium or large data controllers and datasets
- *Do:* threat analysis and organizational improvements

III. Moderate breach, human oversight/technical mistakes

- *What:* database leaks, unauthorized sending of data, unencrypted data on websites, system misconfigurations
- *Where:* mid-scale data controller with minimal or no technical staff
- *Do:* establish protocols and processes for data handling

IV. Low tech breach, human mistakes

- *What:* wrong email attachments, unattended computers, improper disposal, email address leaks
- *Where:* smaller organizations or an individual
- *Do:* advanced data handling systems are unnecessary/impossible; instead, improve awareness and good data practices

⚠

- System reset, restore, restart
- Platform and version migrations
- Outsourcing or shared work on parts of a system

5. Legal analysis

Depending on ontology values, we mark certain DPA analysis points:

I. DPA analysis of cases

- *How:* investigation of factual and substantive elements
- *Why:* description of GDPR infringement and/or data breach
- *Result:* imposition of fine depending on (ontology categories → scalable risk-based approach)
- *Do:* propose technical and organizational measures

II. Applied risk-based approach

- *How:* legal analysis of risk and fine imposition follow the technical analysis classes
- *Why:* risk-based approach → data processing only if risk is not too high or can be sufficiently managed
- *Result:* scalable risk-based approach: the greater the risk and imminent harm, the greater the fine; even if no data breach but merely GDPR infringement

III. Proposed rights-based approach

- *How:* in-depth examination of how risks may lead to specific harms and/or compromise fundamental rights
- *Why:* safeguard the essence of data protection as a fundamental right, as the epicenter of GDPR compliance assessment
- *Do:* apply rights-based approach instead of/in addition to risk-based approach

6. Limitations & future directions

- Manual annotation process → automatic text analysis (AI)
- Small (current) sample size → scale through automation

* available on gdprhub.eu