Politecnico di Torino

PRIMA

PRivacy Infringements Machine-Advice

Final conference

12 January 2026, Bologna

Legal Analysis and Gold Standards for Privacy Policies

Maria Samantha Esposito
Alessandro Mantelero

POLITO
WP2: TECHNO-LEGAL FRAMEWORK AND BEST PRACTICES

- **Focus of the research**

Analysis of **legal requirements**, **recurring criticalities** and **good practices** in GDPR-compliant privacy policies

- **Objectives**
  - Clarify the **meaning, content and practical scope** of GDPR information obligations
  - Support the **development of AI-based systems** for privacy policy analysis, including document evaluation, annotation and training dataset construction
  - Provide a **legal reference standard** for lawful and fair privacy policies

- **Sources examined**
  - **GDPR**, in particular Articles **12, 13 and 14**
  - Guidelines and opinions of the **European Data Protection Board and the Article 29 Working Party**
  - Guidelines by **national data protection authorities**
  - **Legal scholarship**
  - **Decisions of data protection authorities and courts**, at national and EU level

- **<u>Main outputs</u>**
  - Model clauses
  - Operational guidelines

Tools designed to support AI-based document analysis, annotation and training datasets

- **<u>Methodological approach</u>**

Classification of information duties according to three core functions:

I. Promoting transparency in personal data processing

II. Supporting the identification of the applicable legal basis for processing

III. Facilitating the exercise of data subjects' rights and informational self-determination

Additional focus:

IV. Communication modalities aimed at ensuring effective understanding

I. PROMOTING TRANSPARENCY IN PERSONAL DATA PROCESSING

- **Identity and contact details of the controller** and, where applicable, of the controller's representative *(Article 13(1)(a) GDPR)*
- **Contact details of the data protection officer**, where applicable *(Article 13(1)(b) GDPR)*
- **Recipients or categories of recipients of the personal data**, if any *(Article 13(1)(e) GDPR)*
- **Intention to transfer personal data to a third country or international organisation, and information on the applicable safeguards or adequacy decision**, where relevant *(Article 13(1)(f) GDPR)*
- **Storage period of the personal data, or the criteria used to determine it** *(Article 13(2)(a) GDPR)*
- **Mandatory or optional nature of the provision of personal data, and consequences of failure to provide it** *(Article 13(2)(e) GDPR)*
- **Categories of personal data concerned** *(Article 14(1)(d) GDPR)*
- **Source of the personal data**, including whether they originate from publicly accessible sources, where applicable *(Article 14(2)(f) GDPR)*

THE IDENTITY AND THE CONTACT DETAILS OF THE CONTROLLER (SELECTED EXAMPLE)

- **Requirements** (selected examples)
  - Clear and **unambiguous identification** of the controller
  - Information **sufficiently detailed** to allow effective identification and contact
  - In cases of joint controllership or corporate groups: **clear identification of all relevant entities and roles**

- **Criticalities** (examples of recurring issues)
  - Ambiguous or overly generic **identification** (e.g. acronyms only)
  - Unclear allocation of roles in **joint controllership arrangements**
  - Unclear identification of the **controller within multinational groups**
  - **Contact details** difficult to find or inadequate
  - Exclusive reliance on **online forms or chatbots**

The identity and the contact details of the controller

- **Remedies** (selected solutions)
  - Provide **complete and distinguishing identification details**
  - Clearly identify **all joint controllers** and explain roles and responsibilities, where applicable
  - Specify the **relevant controller by geographical area**, where applicable
  - Make contact details **clearly visible and properly labelled**
  - Ensure at least **one effective electronic contact channel**
  - Use online forms/chatbots only as **supplementary tools**

Illustrative examples of model clauses

- **Contact details of joint controllers (where applicable):**

MODEL CLAUSE

Who we are and how to contact us

Your personal data is processed under the joint controllership of Company X S.p.A., with its registered office at Via XXX 100, 00100 Rome, Italy, and Company Z S.r.l., with its registered office at Via XXXX 50, 20100 Milan, Italy. The two companies have determined, by means of a specific arrangement pursuant to Article 26 GDPR, their respective roles and responsibilities with regard to the processing of your personal data.

With respect to their respective roles and responsibilities, Company X S.p.A. is responsible for XX [*e.g., collecting and storing your personal data*], whereas Company Z S.r.l. is responsible for XX [*e.g., managing requests concerning the exercise of your rights as a data subject*]. Both companies cooperate to ensure that the processing of your personal data is carried out in full compliance with applicable data protection laws.

For any queries concerning the processing of your personal data under joint controllership, you may contact Company X S.p.A. at privacy@companyx.com or Company Z S.r.l. at privacy@companyz.com.

- **Contact details of controllers by geographical area (corporate groups):**

MODEL CLAUSE

Who we are and how to contact us

Our company is part of a corporate group that operates through different legal entities. Depending on your place of residence, the responsibility for processing your personal data is assigned to the entity of the group that manages services in your region.

For users located within the European Union, the Controller is Company X S.p.A., with its registered office at Via XXX 100, 00100 Rome, Italy. For users located outside the European Union, the Controller is Company Y Ltd., with its registered office at 123 XXX Street, London, United Kingdom.

For any queries regarding the processing of your personal data, you may contact Company X S.p.A. at privacy@companyx.com or Company Y Ltd. at privacy@companyy.com, depending on your place of residence.

II. SUPPORTING THE IDENTIFICATION OF THE APPLICABLE LEGAL BASIS FOR PROCESSING

- **Purposes of the processing and the corresponding legal basis** *(Article 13(1)(c) and Article 14(1)(c) GDPR)*
- **Legitimate interests pursued by the controller or a third party, where processing is based on Article 6(1)(f)** *(Article 13(1)(d) and Article 14(2)(b) GDPR)*

THE PURPOSES OF THE PROCESSING AND THE LEGAL BASIS (SELECTED EXAMPLE)

- **<u>Requirements</u>** (selected examples)
  - Clear and **specific indication of the purposes** of the processing
  - **Identification of the applicable legal basis** for each purpose
  - Clear links between purposes, legal bases, processing operations and categories of personal data
  - Information detailed to allow data subjects to assess **necessity, proportionality and potential impact** of the processing

- **<u>Criticalities</u>** (examples of recurring issues)
  - Legal basis **unclear, overly broad, or ambiguously** defined
  - Purposes described in **vague or generic terms** (e.g. *improving services*, *research*, *product development*)
  - Use of **standardised or generic expressions** (e.g. *monitoring*, *personalised ads*, *audience insights*), without explaining the specific processing involved
  - **Confusion** between purposes and legal bases
  - Purposes, legal bases and processing operations presented as **separate lists**, without a clear explanation of their relationship

The purposes of the processing and the legal basis

- **<u>Remedies</u>** (selected solutions)
  - Clearly indicate, **for each processing purpose**, the corresponding legal basis
  - Establish a **direct and transparent link** between purposes, legal bases and processing operations
  - Describe purposes in a **clear, specific and contextualised manner**, avoiding indeterminate wording
  - Specify **which categories of personal data** are processed for each purpose and under each legal basis
  - Present purposes, legal bases, data categories and activities in a **structured and coherent way**

Illustrative examples of model clauses

- **Purposes and legal bases**

MODEL CLAUSE

Purposes and legal bases for processing

Each processing activity is based on one of the legal grounds provided by the GDPR, which determine when and how personal data may lawfully be processed.

We process your personal data for the purposes listed below. For each processing activity, we clearly indicate the corresponding legal basis under Article 6 of the GDPR, the categories of personal data involved, and – where relevant – the method of processing:

- **Account registration and access**

To create your personal account and allow you to access the reserved area.
Legal basis: Performance of a contract (Article 6(1)(b) GDPR)
Data processed: Identification data, contact details, login credentials.

- **Customer support**

To handle your enquiries and provide technical or administrative assistance.
Legal basis: Performance of a contract (Article 6(1)(b) GDPR)
Data processed: Contact details, communication records.

- **Legal and regulatory compliance**

To comply with legal obligations, including tax and accounting requirements.
Legal basis: Compliance with a legal obligation (Article 6(1)(c) GDPR)
Data processed: Invoicing details, payment data, identification data.

- **Service improvement**

To analyse aggregated usage data in order to enhance the functionalities of app X. Legal basis: Legitimate interest (Article 6(1)(f) GDPR)
Data processed: Technical data, usage statistics.
Method of processing: Aggregated analysis.

- **Personalised marketing**

To send promotional communications tailored to your preferences and interests.
Legal basis: Your consent (Article 6(1)(a) GDPR)
Data processed: Contact data, preferences, behavioural data (e.g. browsing history, past purchases).
Method of processing: Profiling.

- **Audience segmentation**

To analyse age, gender, and location data for the purpose of tailoring advertising campaigns.
Legal basis: Your consent (Article 6(1)(a) GDPR)
Data processed: Demographic data, device location, behavioural data.
Method of processing: Profiling.

- **Advertising performance measurement**

To evaluate the effectiveness of advertising campaigns (e.g. impressions and click-through rates).
Legal basis: Legitimate interest (Article 6(1)(f) GDPR)
Data processed: Interaction data, browsing activity.
Method of processing: Analytics of impressions and click-through rates.

Alternatively

Provide the information in a structured format (example of table):

Purpose of Processing	Legal Basis	Categories of Personal Data	Methods of Processing (where relevant)
Account registration and access	Performance of a contract (Art. 6(1)(b) GDPR)	Identification data, contact details, login credentials	–
Customer support	Performance of a contract (Art. 6(1)(b) GDPR)	Contact details, communication records	–
Legal and regulatory compliance	Compliance with a legal obligation (Art. 6(1)(c) GDPR)	Invoicing details, payment data, identification data	–
Service improvement	Legitimate interest (Art. 6(1)(f) GDPR)	Technical data, usage statistics	Aggregated analysis
Personalised marketing	Consent (Art. 6(1)(a) GDPR)	Contact data, preferences, behavioural data (browsing history, past purchases)	Profiling
Audience segmentation	Consent (Art. 6(1)(a) GDPR)	Demographic data, device location, behavioural data	Profiling
Advertising performance measurement	Legitimate interest (Art. 6(1)(f) GDPR)	Interaction data, browsing activity	Analytics of impressions and click-through rates

III. FACILITATING THE EXERCISE OF DATA SUBJECTS' RIGHTS AND INFORMATIONAL SELF-DETERMINATION

- **The existence of the rights to access, rectification, erasure, restriction, objection, and data portability** *(Article 13(2)(b) and Article 14(2)(c) GDPR)*
- **The existence of automated decision-making, including profiling, and meaningful information on its logic, significance, and envisaged consequences** *(Articles 13(2)(f) and 14(2)(g) GDPR)*
- **The existence of the right to withdraw consent at any time, where processing is based on consent** *(Article 13(2)(c) and Article 14(2)(d) GDPR)*
- **The existence of the right to lodge a complaint with a supervisory authority** *(Article 13(2)(d) and Article 14(2)(e) GDPR)*

INFORMATION ON DATA SUBJECTS' RIGHTS (SELECTED EXAMPLE)

Requirements (selected examples)

- Information on the rights of **access, rectification, erasure, restriction, objection and data portability**
- Where applicable, information on the **right to withdraw consent**
- Information on the **right to lodge a complaint** with the competent supervisory authority
- Information on data subjects' rights **clearly linked to the specific processing carried out**, enabling concrete understanding and informed exercise of those rights

- **Criticalities** (examples of recurring issues)
  - **Lack** of any information on data subjects' rights
  - Reference to GDPR data subjects' rights **without any link** to the specific processing
  - Lack of explanation of the **nature** of the rights and **the consequences** of exercising them
  - Missing or unclear information on **how rights can be exercised in practice**
  - Insufficient information on **the right to lodge a complaint**, including failure to identify the competent supervisory authority

- **<u>Remedies</u>** (selected solutions)
  - Tailor information on rights to the **specific processing context**, avoiding generic lists
  - Include a **brief and clear explanation** of the relevant data subjects' rights
  - Clearly indicate **how these rights can be exercised**, including:
    - available channels
    - contact points
    - response timelines
- Inform data subjects of their **right to lodge a complaint** with the competent supervisory authority (in their Member State of residence, place of work, or place of the alleged infringement)
- Where applicable, inform data subjects of their right to **seek judicial remedies**

Illustrative examples of model clauses

- **Information on data subject rights**

MODEL CLAUSE

Your rights regarding your personal data

As a user of our online platform, you have the right to access your personal data processed within your personal account area, including your profile information, order history, and saved preferences. You may also request the rectification of inaccurate or outdated information (e.g. a change of email address or billing details).

If you no longer wish to use our services, you may request the erasure of your account and associated personal data. Please note, however, that we may retain certain data for the period necessary to comply with our legal obligations (such as tax or anti-fraud regulations) or to exercise or defend legal claims.

In certain cases, you may also object, under the conditions set out in Article 21 GDPR, to the use of your data for direct marketing purposes, including profiling related to such marketing. If you object, your data will no longer be used for that purpose.

For a detailed description of your rights and the conditions under which they may be exercised, please refer to [*Section X (link)/Annex 1 (link)/our dedicated webpage (link)*].

- **Right to lodge a complaint with a supervisory authority and to seek judicial remedy**

MODEL CLAUSE

Your right to lodge a complaint and seek judicial remedy

You have the right to lodge a complaint with a supervisory authority if you believe that the processing of your personal data infringes the GDPR. You may submit the complaint to the supervisory authority in the Member State of your habitual residence, your place of work, or the place where the alleged infringement took place.

In addition, you have the right to an effective judicial remedy if you consider that your rights under the GDPR have been infringed as a result of the processing of your personal data in violation of the Regulation.

IV. COMMUNICATION MODALITIES AIMED AT ENSURING EFFECTIVE UNDERSTANDING

- **Provided in a concise, transparent, intelligible, and easily accessible form** *(Article 12(1) GDPR)*
- **Communicated in clear and plain language, particularly where addressed to children** *(Article 12(1) GDPR)*
- **Provided in writing or by other means, including electronic means; orally upon request** *(Article 12(1) GDPR)*

Accessibility of privacy policies (selected example)

- **<u>Requirements</u>** (selected examples)
  - Information must be **immediately available or easily identifiable**
  - It must be **clear where and how** the privacy policy can be accessed
  - Accessibility must be ensured **across different interfaces and contexts**
  - Controllers have a **positive obligation** to organise and structure information so as to facilitate access to it

- **<u>Criticalities</u>** (examples of recurring issues)
  - Information **difficult to locate** due to complex structure or layout
  - Privacy policies placed in **hard-to-reach** sections of the interface
  - Information spread across **unrelated or external documents**
  - Use of design choices that can be linked to **deceptive ("dark") patterns**, such as:
    - Hiding relevant information or controls
      (e.g. "Hidden in plain sight", "Left in the dark")
    - Visual or structural choices that obscure privacy-relevant content
    - EDPB (2023). *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them* (v. 2.0)

ACCESSIBILITY OF PRIVACY POLICIES (SELECTED EXAMPLE)

- **Remedies** (selected solutions)
  - Ensure **direct and immediate access** to the privacy policy
  - Use **direct hyperlinks, QR codes or contextual access points** leading to relevant sections
  - Ensure that hyperlinks point **directly to the relevant content**
  - Improve **visibility through layout and design choices**, including clear structure, distinct sections and lists
  - Avoid interface and design solutions that may **obscure essential information or controls**

Illustrative examples of model clauses

- **Enhancing accessibility of privacy information**

OPERATIONAL GUIDELINES

- Implement direct and clear access points to privacy content, such as:
  - Clickable direct links in relevant sections or email footers,
  - QR codes in physical documents or displays,
  - FAQ sections addressing common privacy questions,
  - Contextual pop-ups or tooltips triggered during form completion,
  - Chatbot interfaces providing guided access to privacy policy information.
- Ensure these tools are clearly visible, prominently positioned, and easy to use across all platforms (desktop, mobile, and print).
- Regularly test accessibility features to verify that users can easily locate and understand relevant privacy information.

- **Hyperlinks to relevant content**

OPERATIONAL GUIDELINES

- Ensure that the privacy policy is accessible at all times, without requiring prior user interaction or expression of interest in the service.
- Place the privacy policy in clearly identifiable and graphically distinct sections.
- Avoid placing privacy information next to unrelated content or in marginal areas of the interface.
- Avoid visual choices that reduce the visibility of the privacy policy link, such as using colours similar to the background.
- Ensure simplified access to the privacy policy on mobile devices, ensuring that the privacy policy can be accessed within no more than two taps.

Politecnico
di Torino

samantha.esposito@polito.it

alessandro.mantelero@polito.it