**Prohibited or Restricted Company Practices (Summarized/Filtered from GDPR Articles 1–99)**

Summary: All useful content is within the first 30 articles; the rest are unrelated to our project.

**Article 7**

Companies must not force users to consent to data processing when it is not necessary.

For example, when registering for an account, if only an email and password are required, the company cannot force the user to agree to the processing of browsing history or location data as a condition.

Users must be able to withdraw their consent at any time, and the process must be as easy as giving it.

Companies must terminate data processing based on that consent after it is withdrawn.

**Article 8**

When providing information society services to children under 16, parental consent is required (can be lowered to 13 by Member States). Companies must make reasonable efforts to verify parental authorization.

**Article 9**

Processing sensitive personal data is prohibited (e.g., race, religion, health, sexual orientation, genetics, biometrics) unless one of the following applies:

Explicit consent is given

Processing is needed for employment/social security

Vital interests are at stake

Non-profit organizations process data of members

The data subject has made the data public

Use in legal proceedings

Substantial public interest

Public health

Scientific, historical, or statistical purposes

**Article 10**

Companies may only process data on criminal convictions and offenses if:

Under the control of official authority, or

Authorized by law and appropriate safeguards are in place.

**Article 13**

When collecting data, the controller must provide the data subject with:

Controller’s identity and contact info

DPO contact (if applicable)

Purpose and legal basis of processing

Legitimate interests if Article 6(1)(f) is used

Recipients or categories of recipients

Whether data will be transferred to third countries/international organizations, and if adequate protection exists

Data retention period or criteria

Right to withdraw consent

Whether data provision is required by law/contract, and consequences of not providing

Whether automated decision-making is involved, including logic and impact

**Article 17**

Companies must delete data when it is no longer needed, under any of these conditions:

No longer necessary for processing

Consent withdrawn with no other legal basis

Data was processed unlawfully

Deletion is required by legal obligation

Data collected from minors for information society services

Exceptions: Data may be retained for freedom of expression, legal compliance, research, public health, or legal claims.

**Article 18**

Companies must restrict processing under certain conditions:

Data accuracy is contested

User opposes deletion but requests limited use

Company no longer needs the data, but user requires it for legal claims

Processing is objected to and awaiting verification

**Article 19**

Companies must inform all third-party recipients about any corrections, deletions, or processing restrictions unless this is impossible or overly burdensome.

**Article 20**

If processing is based on consent or contract and conducted automatically, companies must not prevent users from transferring their data to another service.

**Article 21**

Companies must stop processing personal data for direct marketing (including profiling) if the user objects.

The right to object must be clearly and separately communicated when first contacting the data subject.

**Article 22**

Companies must not make decisions based solely on automated processing that have legal or significant effects on individuals.

Exceptions:

Necessary for a contract

Authorized by law with safeguards

Based on explicit consent

Even in these cases, companies must allow human intervention, enable users to express opinions, and contest decisions.

**Article 24**

Companies must implement appropriate technical and organizational measures based on the nature and risk of processing to demonstrate GDPR compliance.

Internal data protection policies should be in place where applicable.

Compliance may be demonstrated through certification mechanisms or codes of conduct.

**Article 25**

Privacy must be embedded into system design and data processing operations (e.g., pseudonymization).

By default, only the minimum necessary personal data should be processed, in terms of amount, scope, retention period, and access.

Data should not be made public by default unless the user actively chooses so.

**Article 30**

Records must include:

Controller’s name and contact details, DPO contact info

Processing purposes

Categories of data subjects and personal data

Data recipients or categories of recipients

Transfers to third countries/international organizations and safeguards

Retention periods or criteria

Technical and organizational security measures

Rationale for Excluding Other Articles:

Irrelevant to the goal: The goal is to extract restrictions on how companies can process personal data and use them to generate risk indicators.

User rights-focused: Some articles focus on individual rights and how to exercise them, rather than on company behavior.

Excessive logical complexity: For example, Article 21(1) involves complex conditional reasoning that's difficult to evaluate without legal expertise.

Not disclosed in privacy policies: e.g., Article 28 concerns contracts between controllers and processors, which users typically don’t see.

Internal compliance duties: e.g., Article 35 on DPIAs — risk assessments that don’t directly relate to user-visible data practices.

Legal procedures or institutions: e.g., Article 45(1) involves decisions by the EU Commission — irrelevant since we are using GDPR as a reference, not as a binding legal source.

Supervisory authorities: Articles after 60 mostly relate to regulators, not end-user transparency.

Penalties for violations: e.g., Article 82 (damages) and 83 (fines) describe consequences of unlawful behavior but are not about restricting data processing itself.