PROMONTORY

EU GDPR: Summary of Key Provisions

After four years of intense negotiations, the European Parliament and the Council of the European Union (the 28 EU member states) on Dec. 14, 2015 reached an informal agreement on the text of the General Data Protection Regulation. The text is still subject to formal votes by the Parliament and Council in early 2016 but the strong expectation is that the current wording will be preserved.

CONSENT

- The data subject's consent means any freely given, specific, informed, and unambiguous indication of the data subject's wishes
- Where consent is relied upon for the processing of special categories of personal data, explicit consent is required
- Parental consent is required for the processing of personal data of children under the age of 16, unless member state law provides for a lower age not under 13

RIGHT TO OBJECT AND PROFILING

- Data subjects have the right to object to processing unless the controller demonstrates compelling legitimate grounds for processing
- Where personal data is processed for direct-marketing purposes, data subjects have the right to object at any time to the processing
- Data subjects have the right not to be subject to a decision based solely on automated processing — including profiling — unless the data subject has given explicit consent, or where the processing is authorized by contract or in law

FURTHER PROCESSING NOT BASED ON CONSENT

- Further processing not based on consent is allowed to safeguard objectives such as: national security; general public interests; the protection of individuals' rights and freedoms; or the prevention, investigation, detection, or prosecution of criminal offenses
- Any further processing not based on consent should consider: the nature of the personal data; the possible consequences of the further processing; and the existence of appropriate safeguards

RIGHT TO ERASURE ("RIGHT TO BE FORGOTTEN")

- Data subjects have the right to request the controller to erase his or her personal data without undue delay where: the data is no longer necessary for the purposes collected; the data subject withdraws consent; or the data subject objects to data processing
- Where the controller has made the data public, the controller shall take reasonable steps to inform the controller processing that data of the erasure request

ONE-STOP SHOP

- Data controllers are regulated by a lead authority located in the territory of their main establishment, although local authorities may deal with local cases
- If a concerned supervisory authority objects to a lead authority's draft decision, the case shall be referred to the consistency mechanism for a binding decision by the European Data Protection Board
- Any EDPB binding decision can be appealed to the Court of Justice of the European Union

DATA PROTECTION OFFICERS

- Controllers and processors shall designate a data protection officer where their core activities consist of the regular and systematic monitoring of personal data or the processing of special categories of personal data on a large scale
- The DPO shall act independently of the controller or processor, reporting directly to the highest management level

DATA BREACH NOTIFICATIONS

- Controllers shall notify the supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours, unless the breach is likely to result in a risk to the rights and freedoms of individuals
- When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller shall communicate the personal data breach to the data subject without undue delay

ADMINISTRATIVE FINES

- Infringements regarding obligations of the controller and the processor may be subject to administrative fines of up to €10 million, or 2% of worldwide annual turnover — whichever is higher
- Infringements regarding the basic principles for processing, data-subject rights, transfers of personal data, or noncompliance with an order by the supervisory authority may be subject to administrative fines of up to €20 million, or 4% of worldwide annual turnover— whichever is higher

PROMONTORY

EU GDPR: Timeline

Four Years of Negotiations

25 Jan 2012 — **EUROPEAN COMMISSION** proposed a new General Data Protection Regulation.

12 Mar 2014 — **EUROPEAN PARLIAMENT** adopted a first reading of the GDPR.

15 Jun 2015 — **COUNCIL OF THE EU** agreed to a general approach on the GDPR.

Jul to Dec 2015 — **INFORMAL TRILOGUE NEGOTIATIONS** occurred between the Parliament, Council, and Commission.

15 Dec 2015 — **INFORMAL AGREEMENT OF THE GDPR COMPROMISE TEXT** agreed following the conclusion of the trilogues.

Path to Formal Agreement*

Jan 2016 — **GDPR COMPROMISE TEXT IS TRANSLATED** into 24 official EU languages by lawyer-linguists.

Late Jan 2016 — **COUNCIL AGREES FIRST READING** either without debate (A-item) or with debate (B-item).

Early Feb 2016 — **EUROPEAN PARLIAMENT VOTES** on the Council's first reading by simple majority. If Parliament approves the Council's position, the legislation is adopted.

Mar to Apr 2016 — **APPROVED TEXT IS PUBLISHED** in the Official Journal of the European Union.

Apr to May 2016 — **GDPR ENTERS INTO FORCE** 20 days after publication in the OJEU. A two-year transition period commences before the GDPR applies.

May 2018 — **GDPR IS APPLICABLE** two years after entry into force.

**Dates may be subject to change.*

STRATEGIC SOLUTIONS TO DATA PRIVACY COMPLIANCE

Promontory's privacy and data protection team draws on a unique combination of privacy expertise and regulatory risk management experience, resulting in practical, workable solutions to help clients meet their regulatory requirements. Our team stays abreast of international regulatory trends and blends experience as former regulators, in-house compliance managers, and global privacy consultants to provide our clients with unique insight. This perspective and expertise allow us to work with clients to maximize the value of data while protecting the rights of individuals and developing practical, proactive solutions that align with regulatory best practices.

CORE SERVICES AND AREAS OF EXPERTISE

- **Strategy, Governance, and Program Implementation**
- **Reports, Reviews, Assessments, and Advice**
- **Incident Preparation and Management**
- **Privacy as a Service**
- **Managing International Obligations**
- **Regulatory Relations**

promontoryprivacy.com **@PromontoryFG**