7 December 2017

Privacy in Europe and the GDPR

An overview

Nicolas Seidler
Senior Policy Advisor
seidler@isoc.org

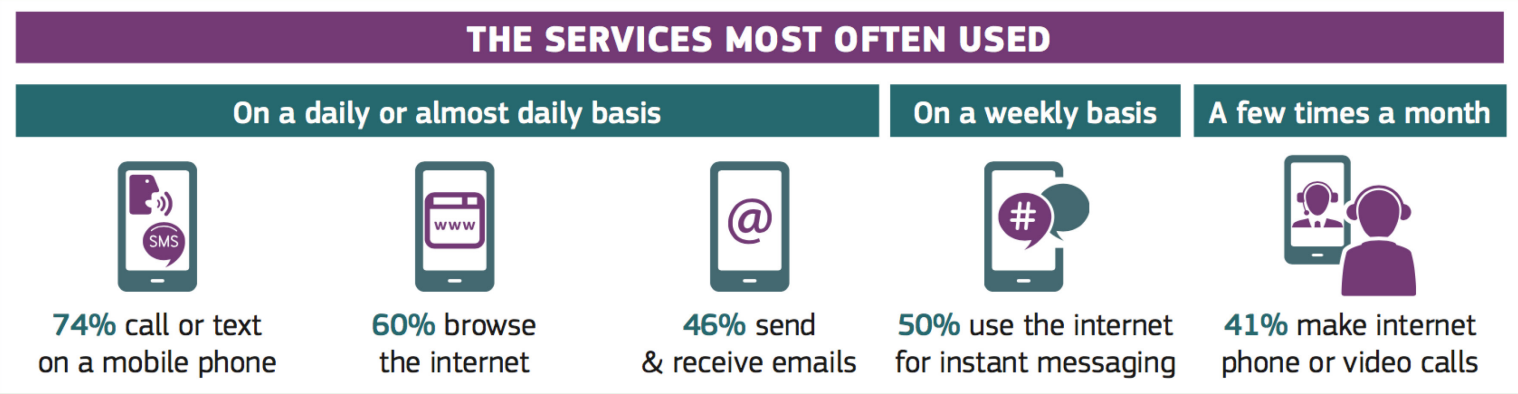
OVERVIEW: EU General Data Protection Regulation

- Privacy context in Europe > EU General Data Protection Regulation (GDPR) > 25 May 2018
- GDPR now recognized as law across EU > 2 years for Member states to ensure implementable in their countries.
- Replaces 1995 Data Protection Directive (DPD) > Internet was in its infancy
- 100+ countries have data protection laws > many modelled after 1995 DPD > same likely for GDPR
- Impact of GDPR: beyond EU. Obligations relate to location of data subject, not data controller. Given cross-border services, will likely generate global consistency around data protection laws.
- Stick: heavy fines for non-complying businesses
- Japan: already in process of convergence and adequacy with GDPR requirements

The privacy: historic context in Europe

Privacy context in Europe

- History: World War 2 and Cold War > surveillance and unchecked use of personal data (e.g. race, ethnicity)
- Consumer protection and regulation against market abuse (e.g. Google, Microsoft)
- High levels of consumer adoption of ICT services and technology



Source: Flash Eurobarometer 433 on ePrivacy, December 2016

Deconstructing the GDPR

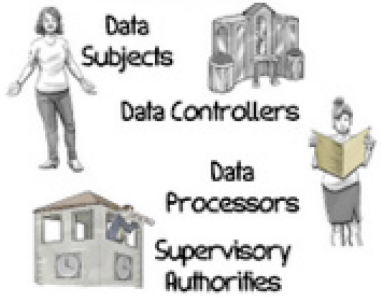
GDPR

TERRITORIAL SCOPE

EU Establishments

Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS



PERSONAL DATA

SENSITIVE DATA

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.

Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.

Data Protection by Design
built in starting at the beginning of the design process

Data Impact Assessment
For high risk situations

LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests

CONSENT

Consent must be freely given, specific, informed, and unambiguous.

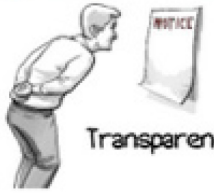
DATA BREACH NOTIFICATION

A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making
"Right not to be subject to a decision based solely on automated processing, including profiling."

Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

ENFORCEMENT

Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:
compensation for material and non-material harm.

INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

GDPR in a nutshell

- 4 years of negotiation
- Adopted in April 2016
- Entering effect on 25 May 2018
- 99 articles setting:
  - **Rights:** for people to access the information companies hold about them
  - **Obligations:** for better data management by businesses
  - **Fines:** for non compliance up to €20 million or 4% of a firm's global turnover

Applicability & scope

Extra-territorial applicability (art. 3 GDPR)

- Individuals, organisations, and companies that are either 'controllers' or 'processors' of personal data will be covered by the GDPR.
- Extraterritorial effects: applies to any entity, no matter its geographical location, which collects or processes the data of people ordinarily resident in the European Union, regardless of:
  - the location of the company processing the data
  - whether the processing takes place in the EU or not
- Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.
- In summary: **it's not about which country you are in, but where the customer is.**

DATA CONTROLLER: A controller is an entity that decides the purpose and manner that personal data is used, or will be used (e.g. bank)

DATA PROCESSOR: The person or group that processes the data on behalf of the controller. Processing is obtaining, recording, adapting or holding personal data (e.g. data center)

Personal data: definition

- Detailed definition of personal data: broadly means a piece of information that can be used to identify a person.
- Extended definition covers for a wide range of personal identifiers (i.e. IP address) to constitute personal data, reflecting changes in technology and the way information is collected
- [New] Pseudonymised personal data can fall within the scope of the GDPR provided that it is sufficient enough to attribute the pseudonym to a particular individual
- Sensitive data (special categories of personal data) specifically include genetic data, and biometric data where processed to uniquely identify an individual

Obligations

Privacy by design (art. 25 GDPR)

- Privacy by design: the inclusion of data protection from the onset of the designing of systems, rather than an addition after the fact.
- GDPR Art 23 calls for controllers to hold and process only the data absolutely necessary for the completion of their duties (**data minimization**), as well as limiting the access to personal data to those needing to act out the processing.

Consent/opt-in (art. 7 GDPR)

Strengthened conditions for consent and explicit opt-in:

- The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent.
- **Consent must be clear** and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language.
- It must be as easy to **withdraw** consent as it is to give it.

Data Protection Impact Assessment (art. 35 GDPR)

- The controller is obliged to carry out a DPIA prior to processing for cases that pose a high risk to the rights and freedoms of natural persons.
- In particular concerning the use of new technologies and systematic evaluation of personal aspects (e.g. profiling, automated processing)
- Includes an assessment of the necessity and proportionality of the processing operations in relation to the purposes.

Data Breach Notification (art. 33 GDPR)

- **Mandatory breach notification** in all member states where a data breach is likely to "*result in a risk for the rights and freedoms of individuals*".
- Notification will be done within **72 hours** of first having become aware of the breach.
- Data processors will also be required to notify their customers and the controllers, "without undue delay" after first becoming aware of a data breach.

Data Protection Officer (DPO) (art. 37 GDPR)

- Mandatory for companies that have "regular and systematic monitoring" of individuals at a large scale or process a lot of sensitive personal data
- Will be main liaison with relevant countries' Data Protection Authorities (DPA)
- DPO must be based in the EU (guidelines exist to define place of establishment)
- One-stop-shop mechanism: if organisation active in multiple EU countries, allows to work with just one DPA in a consistent manner across the EU (same benefits for data subjects)
- Overall objective: turn data protection and privacy into a boardroom issue

Transfer of data to third countries / adequacy (art. 45 GDPR)

- Transfer of personal data to third countries and international organisations can only be made **where adequate level of privacy protection exists**
- The overall evaluation does not require a level of protection identical to that offered within the EU, but requires a level of protection that is "*essentially equivalent*".
- Once an adequate level of protection is recognized by the EU Commission, transfers can be made without specific authorizations
- In the absence of an adequacy decision a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. (e.g. EU-US Privacy Shield)
- **Japan**: advanced process to have formal adequacy with EU data protection laws by early 2018. Could be first in Asia to be given adequacy status.

Rights

Rights to access (art. 15 GDPR)

- Data subjects have the right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose (transparency).
- The controller shall also provide a copy of the personal data, free of charge, in electronic format.
- = crucial change for data transparency and empowerment of data subjects.

Data portability (art. 20 GDPR)

- Right for a data subject to receive the personal data concerning them in a 'commonly used and machine readable format’.
- Only applies portability to data provided by the data subject (e.g. leaves out inferred data or personal data added by others)
- Gives the right to to transmit those data to another controller without hindrance from the controller
- Direct transfer of data from one controller to another “where technically feasible”

Right to erasure (art. 17 GDPR)

Gives individuals the power to get their personal data erased in some circumstances.

This includes:

- where it is no longer necessary for the purpose it was collected
- if consent is withdrawn
- if it was unlawfully processed

Controllers are required to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Penalties

Penalties (art. 83)

- Organizations in breach can be fined up to 4% of annual global turnover or €20 million (whichever is greater)
- A tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment.
- Applicable to both controllers and processors.

Challenges

Challenges

- Enforcement (e.g. Right to erasure > can you really remove something from the Internet?)
- Cost of measures
- Limitations for data intensive innovations (e.g. AI)
- Coverage of data not provided by the individual
- Is regulation the right tool? What about ethics?

Next steps

GDPR: Compliance assessment

- Compliance assessment for businesses dealing with EU personal data
- Also for Internet technical players (e.g. ICANN and WHOIS)
- In doubt, **get legal advice!**

ePrivacy regulation in Europe

- Intended to complement and particularize the GDPR on electronic communications
- To replace E-Communications Privacy Directive
  - Originally set the obligations for telecom operators and ISPs to ensure communications privacy with regard to the services they provide.

Key changes:

- OTT providers are being covered along with traditional telecoms operators and ISPs (e.g. Skype)
- Alignment and synergies with GDPR around data breaches, transparency, etc.
- Opt-in regime is adopted for unsolicited commercial communications

Thank you.

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120