6 October 2017

# EU General Data Protection Regulation

Ukrainian IGF 2017, Kiev

# The EU General Data Protection Regulation (GDPR)

- Replaces the Data Protection Directive 95/46/EC, bringing fundamental changes
- Designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy
- Enforcement date: 25 May 2018 - organizations in non-compliance to face heavy fines

# GDPR

## Key changes brought by the Regulation

# Definitions

- More detailed definition of personal data, providing 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 (Art 4)
- 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
- Applicable to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria
- Sensitive data (special categories of personal data) specifically include genetic data, and biometric data where processed to uniquely identify an individual (Art 9)
- Personal data relating to criminal convictions and offences are subject to additional safeguards for processing (Art 10)

# Extra-territorial applicability (GDPR Art. 3)

- Extended jurisdiction: the GDPR applies to all data processors and controllers processing personal data of data subjects residing in the Union, regardless of
  - the location of the company processing the data
  - whether the processing takes place in the EU or not
- The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to:
  - offering goods or services to EU citizens (irrespective of whether payment is required)
  - and the monitoring of behaviour that takes place within the EU.
- Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

# Consent (GDPR Art. 7)

Strengthened conditions for consent:

- 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.

# Breach Notification (GDPR Art. 33)

- **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, the controllers, "without undue delay" after first becoming aware of a data breach.

# Right to Access (GDPR Art. 15)

- Data subjects have the right for to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.
- 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.

# The Right to be Forgotten (GDPR Art.17)

- The right to be forgotten entitles the data subject to have the data controller
  - erase his/her personal data,
  - cease further dissemination of the data,
  - and potentially have third parties halt processing of the data.
- The conditions for erasure specified, including:
  - the data no longer being relevant to original purposes for processing,
  - or a data subjects withdrawing consent.
- Controllers are required to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

# The Right to be Forgotten
## *- Case Law -*

**ECJ judgment on Google v AEPD, 2014**

"*An internet search engine operator is responsible for the processing that it carries out of personal data which appear*

*on web pages published by third parties*

*Thus, if, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results*"

# The Right to be Forgotten
## *- Case Law -*

- **<u>ECJ judgment on CCIAA Lecce v Salvatore Manni (2017):</u>** "*there is no right to be forgotten in respect of personal data in the companies register*"
- **<u>Belgium Court of Cassation judgment on Olivier G v Le Soir (2016):</u>** "*Right to be forgotten extends to newspaper archives*"
- **Upcoming ECJ judgment regarding a fine issued by CNIL (France) to Google to determine whether 'right to be forgotten' can stretch beyond EU**

# Data Portability (GDPR Art. 20)

- GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which
  - they have previously provided in a 'commonly use and machine readable format' and
  - have the right to transmit that data to another controller.

# Privacy by Design (GDPR Art. 25)

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

# Data Protection Officers(GDPR Art. 37)

- Under GDPR instead of submitting notifications / registrations to each local DPA or to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs), there will be internal record keeping requirements for processors/controllers
- DPO appointment will be mandatory only for those controllers and processors whose core activities consist of
  - processing operations which require regular and
  - systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

# Data Protection Officers

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

# Penalties (GDPR 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.

# Data Protection Impact Assessment (GDPR Art. 35)

- 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.
- Particularly required for
  - a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
  - processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
  - a systematic monitoring of a publicly accessible area on a large scale.
- Prior consultation with the Supervisory Authority is required if the DPIA shows that the processing carries high risk

# Transfer of Data to Third Countries (GDPR Art. 45)

- Transfer of personal data to third countries and international organisations can only be made where adequate level of protection exists
- Adequacy decision shall be made my the Commission (to be published in OJ and its website as a list, continuous monitoring required)
- 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.

# GDPR

Global Impact-Final Remarks

# Impact of the GDPR on Businesses from non EU-Member States

- Broadened territorial scope:
  - Non-EU data businesses offering goods or services (paid or unpaid) to EU residents must comply with the GDPR obligations
  - Appointing a representative in the EU (a DPO)
  - Data Protection Impact Assessment
  - Compliance to GDPR principles, consent requirement, privacy by design ect.
  - Heavy penalties in case of non compliance
- Businesses from non EU member states might be denied transfer of data due to lack of adequate protection or appropriate safeguards

# 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