DLA PIPER

Edu brief for American Chamber of Commerce

The EU General Data Protection Regulation (GDPR) in 20 Questions

16 February and 17 May 2016

Stanislav Bednar

1. Why all the buzz around the EU General Data Protection Regulation?

- One law, **directly applicable** in all 28 Member States.
- Replaces the **1995** Data Protection Directive and the national laws transposing the Directive.
- Will apply from **2018** – national laws apply until then.
- Big picture implications: Will the EU continue to lead the way in personal data protection?

2. Has it been adopted now? Are these really the final rules?

- **Last week**
  - 17 December: EP LIBE endorsed the texts agreed in the trilogues.
  - 18 December: COREPER confirmed the final compromise texts.
- **Spring 2016**
  - Legal-linguistic review of the texts
  - Adoption by the EU Council and Parliament
  - Publication in Official Journal on 4 May 2016
  - regulation entered into force on 25 May 2016
- **2016-2017**
  - Delegated acts/implementing acts
- **Spring 2018**
  - Application of the rules from 25 May 2018

3. To whom does it apply?

- Processing of personal data in the context of the **activities of an establishment of a controller or a processor in the Union**, regardless of whether the processing itself takes place within the EU.
- Processing of personal data of **data subjects who are in the Union** by a controller or processor **not established in the Union** where the processing activities are related to the **offering of goods or services** to data subjects in the European Union **irrespective** of whether a **payment** of the data subject is required, or related to the **monitoring of the behaviour** of such data subjects as far as their behaviour takes place within the EU.

4. Do the principles stay the same or are we starting over?

- Personal data must be processed **lawfully, fairly** and in a **transparent manner**.
- Personal data must be processed for **specified, explicit** and **legitimate purposes** and not further processed in an incompatible way.
- Personal data must be **adequate, relevant** and **limited** to what is necessary in relation to the purposes.
- Personal data must be processed in a way that ensures **appropriate security** using appropriate technical or organizational measures.

And a new principle: The controller shall be responsible for and **be able to demonstrate compliance** with the principles.

5. How large are the fines likely to be?

- Graduated approach – **up to 4% worldwide turnover maximum**.
- Due regard is to be given to:
  - the **nature, gravity and duration** of the infringement;
  - the **intentional character** of the infringement;
  - **degree of responsibility** (e.g. data protection by design or by default) or any relevant **previous infringements**;
  - **cooperation with the supervisory authority** (and the manner in which supervisory authority learned of infringement);
  - **categories of personal data** affected;
  - **other aggravating or mitigating factors** (e.g. financial benefits, etc.)

6. Will international data transfers be affected?

- Same philosophy as before i.e. only under very strict conditions:
  - **Adequacy** decisions by Commission.
  - **Appropriate safeguards**, such as standard data protection clauses
  - **Derogations**: Explicit consent/necessary for performance of the agreement/…
  - What about **legal disclosure** obligations?
    - "*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty.*"

7. Will we need to appoint a DPO or not?

- Yes and No! - DPO to be designated when the core activities of the controller / processor:
  - require regular and systematic **monitoring of data subjects on a large scale**;
  - consists of processing on a large scale of **"special categories of data"** (Art. 9) or data relating to **criminal convictions**.
- A group of undertaking may appoint a **single DPO.**
- A DPO may be a **staff member or a consultant** (service contract), to report to the highest management level.

8. How will one-stop-shop change our compliance program?

- One-stop-shop relevant to interactions with supervisory authorities in relation to **cross-border processing**.
- Definition of cross-border processing could be clarified, even if the intent is clear.
- With respect to its cross-border processing, the controller or processor will deal only with its **lead supervisory authority**.

9. What to do in case of a data breach?

- Notification to the supervisory authority without undue delay and where feasible **no more than 72 hours,** unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.
- Reasoned justification in case breach is not notified within 72 hours.
- **Data subjects shall be notified without undue delay** if the breach is likely to result in a high risk for the rights and freedoms of individuals to allow them to take the necessary precautions.
- Communication to the data subject is not required in certain cases.

10. Can we still process personal data on the basis of consent?

- Yes, **but**:
  - consent should be **freely** given, **specific**, **informed** and **unambiguous**;
  - by a **statement** or **clear affirmative action**;
  - Controller has **burden of proof**.
- In practice for example a ticking a box
- Contract performance cannot be made conditional to consent, if processing is not necessary.

11. Can we still process personal data on the basis of legitimate interests?

- Yes – **with some changes**:
  - Obligation to specifically inform data subjects.
  - Data subject entitled to require restriction of processing of his/her data while verifying if fundamental rights don't override legitimate interests.
- **Examples**: Preventing fraud; ensuring network and information security.
- Direct marketing purposes may be regarded as carried out for a legitimate interest?

12. Will data collection from kids become illegal?

- No - General principles of lawfulness of processing (Art. 6) shall apply.
- **Processing of personal data of a child below the age of 16 years requires the consent** (given or authorized) **by the parent** (or other holder of parental responsibility).
- Member States can lower the age threshold (but not below 13 years).
- The controller shall make **reasonable efforts to verify** that consent is given or authorized by the holder of parental responsibility over the child.

13. Will individuals get new rights?

- Yes – several new and expanded rights.
- Data **portability.**
- **Restriction** of processing.
- Expanded right of erasure - the **Right To Be Forgotten.**
- Rights regarding **profiling**: *using data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interest, reliability, behaviour, location or movements.*

14. Will we get new types of sensitive data?

- **General rule** - prohibition to process personal data, revealing:
  - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, **genetic data**, **biometric data** in order to uniquely identify a person or data concerning health or sex life and sexual orientation.
- But **10 exceptions** apply (explicit consent, etc.)
- **Beware**!
  - Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data.

15. Does the Regulation still apply if anonymise our data?

- Information that does not relate to an identified or identifiable natural person, or data rendered anonymous in such a way that the data subject is not or no longer identifiable, **will not be subject to the Regulation**.
- Data that has undergone **pseudonymisation**, which could be attributed to a natural person by the use of additional information, is personal data subject to the Regulation.
- To determine whether a person is identifiable, account should be taken of all the means **reasonably likely** to be used, looking at all **objective** factors, such as the costs and amount of time required, available technology at the time of the processing, and technological developments.

16. When will we need to conduct a privacy impact assessment?

- When using new technologies and likely to result in a risk for the rights and freedoms of individuals. In particular:
  - **systematic and extensive evaluation of personal aspects based on automated processing** (including profiling) and on which decisions are made, significantly affecting the individual.
  - **large scale processing of "special categories of data" or criminal data**.
  - **systematic monitoring of a publicly accessible area** on a large scale.
- Supervisory authority to publish a list of operations subject (and not subject) to impact assessment.
- Assessment review when risk changes.

17. We've always acted as a processor – what will our liability be?

- **Direct claims**: data subject can lodge a complaint directly against a P (administrative as well as judicial).
- **Qualified liability**: A P shall be liable for the damage caused by the processing **only** where it has not complied with obligations of this Regulation specifically directed to Ps or acted outside or contrary to lawful instructions of the C.
- **Burden of proof**: A C or P shall be exempted from liability if it **proves** that it is not in any way responsible for the event giving rise to the damage.
- **Liable for sub-processors**: Where that other P fails to fulfil its data protection obligations, the initial P shall remain **fully liable** to the C for the performance of that other processor's obligations.

18. Is it true the G29 will be dissolved?

- An independent body of the Union with legal personality – the **European Data Protection Board** – will be established.
- Will **replace** the Article 29 Working Party.
- Empowered to issue binding decisions.
- Decisions subject to action for annulment before the Court of Justice of the European Union.

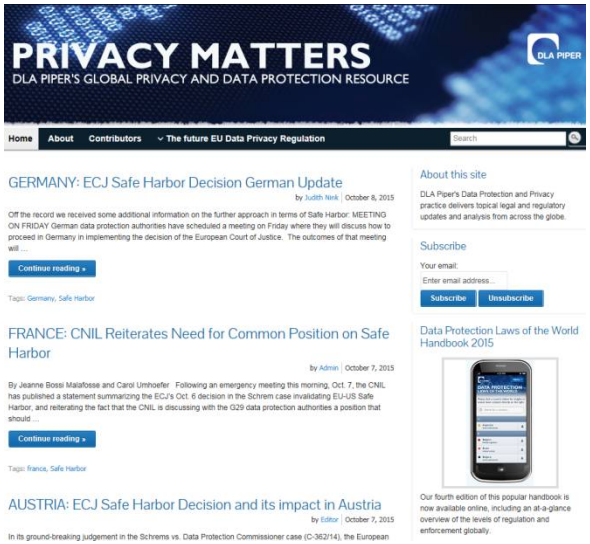
19. Will the regulators be issuing guidelines or recommendations?

- The Commission will be granted implementing powers.
  - **Implementing acts:**
    - approved codes of conduct;
    - technical standards for certification mechanisms and data protection seals and marks;
    - third country adequacy decisions;
  - **Delegated acts:**
    - information to be presented by the icons;
    - requirements for the data protection certification mechanisms.

20. How far does harmonization really go?

- Member State law should reconcile rules governing **freedom of expression and information** with the protection of personal data.
- Member State law or collective agreements may provide for specific rules on **employee personal data processing**.
- Member States may adopt specific rules if necessary to reconcile the right to the protection of personal data with an **obligation of professional secrecy**.

Stay Informed



Subscribe to our **Privacy Matters blog** for regular updates

http://blogs.dlapiper.com/privacymatters/

Access our

Data Protection Laws of the World Handbook at

www.dlapiperdataprotection.com

New edition to be released Q1 2016