17 December 2015

EU General Data Protection Regulation:

The outcome of the negotiations ("trilogues") and 10 key points

Lead European Parliament Committee:
Committee on Civil Liberties, Justice and Home Affairs (LIBE)

Rapporteur: Jan Philipp Albrecht MEP, Greens / European Free Alliance

Better data protection for everyone in the EU – From the 1995 Directive to the 2015 Regulation

Problem: A privacy patchwork. Until today, the 28 EU member states of the European Union enact their own laws based on the 1995 Data Protection Directive. Despite the fundamental principles enshrined in Article 16 of the Treaty on the Functioning of the EU (TFEU) and Article 8 of the Charta on Fundamental Rights (CFR), different implementation and enforcement of the Data Protection Directive throughout the Member States have led to **different data protection standards** with negative consequences for citizens and businesses across the single European market.

Solution: The same, high data protection level for all 500 million EU citizens. The Regulation will apply to all data processing by individuals as well as private and public entities. Only the prevention, investigation, detection and prosecution of criminal offences and the enforcement of criminal penalties are excluded from the latter area of the scope and will fall instead under the future **Directive on data protection in the police and justice sector**. This act has been negotiated and concluded in parallel to the Regulation.

The new Data Protection Regulation aims at establishing a **single level playing field on the basis of high data protection standards**, fit for the digital age. As part of the EU's Digital Single Market it will make it easier for data controllers and users to know what their rights and obligations are and to enforce their rights. Companies can no longer have their main centre of operation in a country with weak data protection standards. According to the Regulation, EU data protection standards apply whenever goods and services are offered on the European market – whether from within or from outside of the EU. Stronger, consistent enforcement measures, new rights like data portability, principles such as data protection by design as well as high sanctions in case of infringements will strengthen the trust of citizens in European data protection and foster competition in the digital market.

Timetable: After the proposal of the Data Protection Regulation in January 2012 by the European Commission, the adoption of the European Parliament's first reading in March 2014 and the Council's general approach (position) in June 2015, trilogue negotiations took place from 24 June until their conclusion on 15 December 2015, when a tentative agreement was found. This has now been confirmed by the Parliament's LIBE committee (17 December) and needs to be passed by the Member States' EU ambassadors in the Council (COREPER) (foreseen for 18 or 21 December). After, there will be formal adoptions at Minister level and by the Parliament's plenary. The regulation will then apply in every EU Member State two years after the publication in the EU's Official Journal.

10 key points

1. Right to be forgotten, data portability and access to data: Whoever wants to request the deletion of his or her personal data will have this “right to be forgotten” vis-a-vis companies like Google, Facebook etc. The data controller will also have to communicate the deletion request to third parties to whom the data has been sent. The regulation guarantees a meaningful balance between freedom of expression and information on the one hand, and the protection of personal data on the other. After the “Google-judgment” of the European Court of Justice in May 2014 that was still based on the 1995 Data Protection Directive, the Regulation now clarifies in which specific cases and under which procedures the right to be forgotten applies. Moreover, the Regulation ensures the right to data portability. If someone wants to change a service, providers have to hand over personal data electronically and in an **interoperable format** on request – quickly and cost-free.

***2. Informed consent as a cornerstone*:** Users must be informed about any processing of their data. They must freely and clearly give their consent to data processing – or reject it. There is no assumed agreement or a simple unticking of pre-ticked boxes. A **clear affirmative action** will be needed for each and every consent. Consent may not be linked to the conclusion of a contract if the data processing is not needed for the respective product or service. Technical standards for automatically objecting to data collection, such as **“do not track”** for websites, can now be made **legally binding**. The Parliament has succeeded in narrowing down the “legitimate interest” of the data controller (which allows for data processing without consent) to what can reasonably be expected by the person affected based on their relationship with the data controller.

3. Right to information and transparency: The Parliament demanded more rights to information and transparency than did the European Commission – and succeeded. Users will now receive clear and concise information on how their data is processed. Data controllers have to explain in an easily understandable way, free of charge, which user data they process in which context, for which purpose, and to whom it is transferred. **EU-wide standardised icons** will explain the long pages of legalistic language in privacy policies.

4. Transfer of data to third countries: The Parliament insisted that companies are not allowed to hand over data from the European Union directly to third countries’ authorities. Data may only be transferred under a **mutual legal assistance treaty** or similar instruments based on EU law. This shield against foreign access to European data was already contained in a first draft of the Commission’s proposal, but deleted after intensive lobbying by the US government. It was raised again by the Parliament after the Snowden revelations. The Commission will have to report regularly on data transfers to third countries. After the European Court of Justice declared the “Safe Harbor” agreement on data transfers to the US invalid (in its Max Schrems-ruling of 6 October 2015), the European Parliament demanded further safeguards and clarifications. Also, in third countries to which EU citizens’ data of is transferred, citizens must have essentially equivalent and effective rights, including **judicial redress**. A third country cannot claim to offer an adequate level of protection if it allows for disproportionate access of authorities to personal data stored in the private sector, as was revealed by Edward Snowden.

5. Future-proof definitions: All information that can be directly or indirectly linked to a person are defined as personal information and are protected. This is even more important in times of “Big Data”. The Parliament has also clarified that data does not necessarily have to reveal the civic identity of a specific person in order to be considered protected – it is enough if it can be used to **“single out”** a person, for example by recognising him or her based on browser settings.

6. Strong sanctions: *Companies found to be* infringing the rules set out in the Regulation will face tough sanctions. The Parliament supported possible sanctions up to **4% of the global annual turnover** for undertakings, **or €20 million** for other data processors. These tough sanctions shall underline that infringements of data protection provisions also constitute violations of fundamental rights. Of course, sanctions always have to be proportionate. Thus they cannot be imposed on small companies in cases of a first, accidental or minor violation.

7. Privacy by Design / Privacy by Default: Data processors have to design their services in a data-minimising way and with the most privacy-friendly pre-settings. Only data necessary for the provision of a service shall be processed. Companies may not make the provision of a service dependent on consent to process additional data that is not needed for this. This means, for example, that a flashlight app on the smartphone can therefore no longer demand access to the address book just for switching on the light. Moreover, it shall be possible to use services anonymously or pseudonymously.

8. Less red tape: Besides the reduction from 28 different standards to one data protection rule for the European market, there are a number of other alleviations foreseen for companies, especially **smaller companies**. The mandatory appointment of a data protection officer (DPO) depends on the amount and relevance of data processing, not on the size of a company. The Parliament has clarified that the data protection officer does not have to be a full-time position and can also be an external contractor. Member States can however provide for stricter rules on appointing a DPO if they wish so.

9. Harmonised enforcement of the rules: A European Data Protection Board, consisting of national data protection authorities, shall ensure the harmonised application of data protection law and be able to take binding decisions for cases of Europe-wide relevance – similar to how it is done already concerning EU competition law and banking supervision. In this way a “race to the bottom” in EU member states with weak law enforcement is no longer possible. The independence of data protection authorities is ensured, the last word was not given to the Commission but to the European Data Protection Board which can now adopt legally binding decisions for the whole European market.

10. One counterpart for all of Europe: The “one-stop-shop” approach means citizens have only one data protection authority in the whole EU to deal with. Citizens can go to their national data protection authority for complaints that cover data abuses anywhere in the EU. Companies will only have to deal with the authority in the country of their main establishment.