7 January 2015

EU General Data Protection Regulation
State of play and 10 main issues

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

Rapporteur: Jan Philipp Albrecht, Greens/EFA

From a Directive to a Regulation

Problem: A privacy patchwork. Currently, the 28 EU Member States enact their own laws based on the 1995 Data Protection Directive. While the fundamental principles, summarized as "informational self-determination" by the German Constitutional Court, are still valid, different laws and implementation have led to different data protection levels across the EU, and enforcement options are very limited.

Solution: Same data protection level for everybody. The proposal for a new data protection regulation aims at high data protection standards, which are better harmonised and fit for the internet age. A unified data protection Regulation that is directly applicable as part of the EU's Digital Single Market will make it easier for data controllers and users to know what their rights and obligations are. Companies could no longer have their main centre of operation in a country with weak data protection standards. Furthermore, the proposal foresees that EU data protection law is valid whenever the European market is targeted – whether from within or outside of the EU. Stronger enforcement rights and principles such as data protection by design will strengthen the trust of citizens and users.in European data protection.

State of play: Waiting for Member States. The EU Commission presented its legislative proposal in January 2012. After intense lobbying which led to 3999 amendments only in the lead Civil Liberties, Justice and Home Affairs Committee, the European Parliament almost unanimously adopted its version of the draft regulation in first reading in March 2014. EU Member States in Council have long been in a stalemate, but since summer 2014 are finally moving towards their general approach. They have agreed on chapters I, IV, V and IX so far, which deal with specific rules for public authorities and other special sectors, obligations for the data controller and processor, and international data transfers. Both Parliament and Council aim for the opening of trilogue negotiations about the final version of the law before the summer break in 2015, and the conclusion of the legislative work by the end of 2015. The Regulation will then be applied in every EU Member State after two years of transition period that allows for everybody to adapt to the new rules.

Main issues

Right to erasure, data access, and correction: Whoever wants to request the deletion of his or her personal data should have this "right to erasure" vis-a-vis firms like Google, Facebook etc. The data controller will also have to communicate the deletion request to third parties to whom the data had been sent. The contested “right to be forgotten” has been limited by the Parliament – only those publishing personal data in breach of data protection law are obliged to ensure every copy is deleted. The regulation demands for a meaningful balance between freedom of expression and freedom of information on the hand, and the protection of personal data on the other. While there is an understanding in Parliament that the “right to be de-listed” as spelt out in the Google Spain judgement of the European Court of Justice in May 2014 is already contained in the text, Member States are still discussing the need to add specific wording on this. Furthermore, providers should hand over personal data to the person it belongs to electronically on request - fast and without any costs.

***Informed consent as a cornerstone*:** Users must be informed about what happens with their data, and they must in principle be able to consciously agree to data processing – or reject it. While the Parliament insists on “explicit” consent as proposed by the Commission, the Council’s version of the draft law foresees the much more vague “unambiguous“ consent, which would give a cheap excuse to data controllers for actually not asking for consent. Technical standards for objecting to data collection, such as “Do not Track” for websites, can be certified at EU level and thereby receive general validity. The Parliament has narrowed down the “legitimate interest” of the data controller (which would allow for data collection and processing without consent) to what can reasonably be expected by the persons affected. Member States on the other side even discuss allowing a change of the purpose of the data processing merely based on “legitimate interest” of the controller. This would weaken the individuals’ rights below what the Commission had proposed.

Right to information and transparency: The Parliament demands more rights to information and transparency than the European Commission. Users should receive understandable information on how their data are processed or if the provider has transferred data to public authorities or intelligence services. Data controllers will have to explain in an easily understandable way, free of charge, which user data they process in which context. Terms of use must be easy to comprehend. In the view of the Parliament, standardised icons should replace long pages of legalistic language in privacy policies.

Transfer of data to third countries: The Parliament insists that companies are not allowed to hand over data from Europe directly to third countries´ authorities. This can only occur under a mutual legal assistance treaty or similar instrument based on European 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 of the American government. It was put back by the Parliament after the Snowden revelations. Member States have not incorporated this approach in their version of the chapter on international transfers, but seemingly are open to it.

Future-proof definitions: All information that can be directly or indirectly linked to a person are defined as personal information and need to be protected. This is even more important in times of "Big Data", where more and more data sets can and will be combined and analysed. Therefore, there should be incentives to use pseudonymised data which cannot be linked to other data. The Parliament has also clarified that data does not necessarily have to (even indirectly) reveal the identity of a specific person in order to be

protected – it is enough if it can be used to “single out” a person from a larger group.

Strong sanctions: In case of illegal data processing and in severe cases, companies should face tough sanctions. The Commission has proposed sanctions of up to two per cent of global annual turnover, and Member States seem to want to stick to this. The Parliament wants to rise the possible sanctions to up to five per cent of the global annual turnover, or 100 Million Euros. Such tough sanctions will discourage companies from considering data protection violations in the first place and will finally ensure the attention of the executive boards for this fundamental right. Of course, sanctions always have to be proportionate, so small companies will not have to fear to be put out of business for a first, accidental or minor violation of data protection laws.

Privacy by Design/Privacy by Default: Data processors, as well as producers of IT systems, should design their services in a data-minimising way and with the most data protection-friendly pre-settings. A strong principle of purpose limitation means that only data necessary for the provision of a service are processed. It should also be possible to use services anonymously or pseudonymously. The Parliament has explicitly prohibited the coupling of providing a service to additional and over-shooting data collection. Member States are currently considering a German proposal that would oblige service providers to offer pseudonymous or anonymous use of their platforms.

Less red tape: According to the European Parliament, the mandatory appointment of a data protection officer (DPO) should depend on the amount and relevance of data processing, not on the size of a company. Prior consultations with the supervisory authorities should be massively reduced, and in exchange the corporate data protection officer should be mandatory above a certain threshold. The Council has suggested leaving it up to the Member States if the data protection officer should be mandatory at all. This is unacceptable for the Parliament, as it would lead again to a race to the bottom. The Parliament on the other side has clarified that the DPO does not have to be a full-time position and can also be an external contractor.

Harmonised enforcement of the rules: A European Data Protection Board, consisting of national data protection authorities, should 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 will not be possible in the future. Parliament and Council agree to this general approach which would not give the last word to the Commission - thereby the independence of data protection authorities is ensured. Member States however are still discussing the details of this “one-stop shop”. All institutions agree that Data Protection Authorities need more resources and staff, including more technical expertise.

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 abuse anywhere in the EU. Companies will only have to deal with the authority in the country of their main establishment.