en | de

News | 18.10.2013

Respect My Privacy

New Data Protection Rules approach first vote

On Monday, 21st October, the Civil Rights, Justice and Home Affairs committee of the European Parliament will have its first vote on new EU wide data protection rules. Although we are still some months away from a final vote, this will give an important signal before negotiations with Member States begin. It has also been a long time coming. With a record breaking over 3000 amendments being submitted by MEPs, many were disappointingly similar to those being pushed by corporations with a financial interest in data processing. The outcome looked grim until the spying revelations of Edward Snowden increased the pressure on right and centre-right MEPs to put citizens first. The draft of these new rules currently contains important protections for European citizens but these could slip away as negotiations continue, making it essential to keep up the current pressure. Below you can find a short description of why we need this reform now, and a summary of the current state of play in 10 points

Same data protection level for everybody

EU Member States currently enact their own laws based on a Directive drawn up in 1995, before mass commercial data crunching was practical, or in some cases even possible. Different laws and implementation have led to different data protection levels across the EU, and enforcement options are very limited. The aim of the current reforms are high data protection standards which are a better fit for the internet age. According to the European Commission's proposal, 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 data of European residents is processed – whether within or outside of the EU.

The Data Protection Regulation in 10 points

1

Right to deletion, data access, and correction: Whoever wants to request the deletion of his or her personal data on the internet, should have this 'right to deletion' vis-a-vis firms like Google, Facebook etc., they also have to communicate the deletion request to third parties to whom they had sent data. Anyone publishing private data illegally, is obliged to ensure every copy is deleted. The report demands for a meaningful balance between freedom of expression and freedom of information on the one hand, and the protection of personal data on the other. Furthermore, providers should explain in an easily understandable way, free of charge, and quickly, what user data they process in what context and hand over these data electronically on request.

2

***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. Terms of use must be easy to comprehend, and standardised icons should replace pages and pages of legalistic language in current privacy policies. Website owners should only be allowed to track users if the privacy settings of the browser signal that the user agrees. Technical standards have to be certified at EU level.

3

Right to information and transparency: The report demands a greater right to information and transparency and, in that way, goes further than the European Commission. Users should receive understandable information on how their own data are being processed or if the provider has transferred data to public prosecution authorities or intelligence services.

4

Transfer of data to third countries: Whistleblower Edward Snowden and the Prism scandal laid the ground for the report's demand: companies like Google are not allowed to transfer data to third countries´ authorities. This can only occur under European law or an agreement based on European law. Without any concrete agreement there would be no data processing by telecommunication and internet companies allowed. This was part of a first draft of the Commission's proposal but deleted after intensive lobbying of the American government. It is back in the draft Parliament report.

5

Future-proof definitions: All information that can be directly or indirectly linked to a person or used to single out a person from a larger group, 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.

6

Strong sanctions: In case of illegal data processing and in severe cases, companies should face tough

sanctions. For larger companies, sanctions could rise to € billions. Tough sanctions will discourage companies from considering data protection violations.

7

Privacy by Design/Privacy by Default: Data processors, as well as producers of IT systems, should design their offers 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.

8

Less red tape: The appointment of a data protection officer 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 in exchange the corporate data protection officer will be mandatory above a certain threshold.

9

Harmonised enforcement of the rules: A European Data Protection Board should ensure the harmonised application of data protection law and be able to make decisions which are now made by national data protection authorities – as is done already concerning EU competition law and EU 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. The new European Data Protection Board should also support national data protection authorities. Data Protection Authorities need more staff and resources.

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 abuse anywhere in the EU. Companies will only have to deal with the authority in the country of their main establishment. In cases of disagreement, the new European Data Protection Board should take the final decision. This should not be left to the Commission in order to safeguard the independence of the data protection authorities.

What's the next step?

21st October

Vote in the Committee on Civil Rights, Justice and Home Affairs ("orientation vote")

As soon as Council has agreed upon a common position:

Starting of negotiations between European Parliament, Council and Commission (“Trilogue”). The Council will meet on 24th and 25th October, with the "Digital Agenda“ to be debated.

Event

Picture of Budapest - Hungary © Jaap Hart

[An honest broker? The Hungarian Council presidency in …]

03.07.2024

Letter

© Alexander Briel

[In Defence of Democracy]

08.05.2024

Press release

https://unsplash.com/photos/a-long-hallway-with-a-bunch-of-lockers-in-it-ihl2Q5F-VYA

[Final report on Hungary shows damning picture on rule …]

24.04.2024

News

European Union

[Plenary Flash 22 - 25 April 2024]

19.04.2024

Responsible MEPs

Jan Philipp Albrecht

Member

Please share

- E-Mail