Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf 26. April 2018

Facebook Privacy Scandal – Enforcing the New Data Protection Law within Social Network Services

In March 2018, it became public that– according to the company – personal data of 87 million users worldwide, of which 2.7 million were Europeans and around 310,000 Germans, were collected through an app which was connected with Facebook from November 2013 until May 2015 and transferred to the analysis company Cambridge Analytica. Apparently, they have been also used for profiling for political purposes there.

On this occasion, the competent authority in Germany, the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI), initiated fine proceedings against Facebook. He is in close exchange with his European colleagues, with the Information Commissioner's Office in Great Britain and the Article 29 Working Party in particular. The privacy scandal concerning Facebook and Cambridge Analytica highlights the handling of millions of users' data. The occurrences regarding Cambridge Analytica are further documenting that Facebook allowed developers of apps access to personal data of individuals who are friends with Facebook users who use this app on a huge scale over years. It happened without consent of the data subjects. In fact, the currently discussed case of a single app is just the tip of the iceberg. Tens of thousands of apps employ the Facebook login system. The number of the persons concerned unlawfully is likely to go dramatically beyond the dimension of the Cambridge Analytica case and, basically, affect all Facebook users. This incident shows, moreover, the risks of profiling when using social media and subsequent microtargeting which, obviously, was utilized for the manipulation of a democratic process of developing an informed opinion.

Germany's Conference of Independent Federal and Länder Data Protection Authorities, commonly referred to as the DSK or "Datenschutzkonferenz" (Data Protection Conference) urges to draw the following conclusions from the infringement of data protection rights of individuals in, obviously, huge numbers:

- Social network services have to adjust their business models to the new European data protection law and have to meet their responsibilities. Among these are: making reasonable arrangements against abuse of personal data.

- Facebook has to reveal the real extent of the opening of the platform for app providers in the years up until 2015 and state reliable numbers of the apps provided and also of the persons affected by the Facebook login system. Data subjects concerned have to be informed about the legal infringements.
- In the future, Facebook has to make sure that the rules of the General Data Protection Regulation (GDPR) are being implemented: the introduction of the automatic facial recognition by Facebook in Europe raised significant doubts if the procedure of approval is compatible with the legal requirements, with regards to consent in particular. It is an illegitimate manipulation of users if Facebook forces them and makes it much easier for them to give their consent in the processing of biometric data than to refrain from it.
- The reactions to the infringement of data protection law are not restricted to the execution of data protection law but are concerning also competition and anti-trust law. The call for demerging the Facebook enterprise will increase to the same extent as it tries to obtain anti-competitive advantages on the market of digital services by systematically bypassing data protection law. There is a demand of European initiatives to limit monopoly-like structures in the area of social networks and to create transparency about algorithms.

Since the processing of data is becoming more and more complex and intransparent for data subjects, the data protection authority is playing a crucial role. Its professional expertise is in demand. They have to have the organizational and personnel means to be able to advise and shape. A strong data protection law and effective supervisory authorities reduce the risks for citizens in a digital society. If Facebook and other social network services are not ready to comply with the European law that protects users, all measures available to the supervisory authorities have to be exploited consistently on the national and on the European level.