KYRIAKIDES GEORGOPOULOS
Law Firm

Dealing with Big Data under the new EU General Data Protection Regulation

December 20, 2016

What is Big Data?

As per the definition given by the European Commission, the term 'Big Data' refers to *"large amounts of different types of data produced from various types of sources, such as people, machines or sensors. (…) Big Data may involve personal data, that is, any information relating to an individual, and can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address*".

Big Data is a recently emerged market the benefits and opportunities of which are still being explored. Following cloud computing and SaaS (software as a service), IT companies are now exploiting this new market challenges as well. It is expected that Big Data Processing shall enable companies to improve the services they provide to customers and increase their productivity in the framework of the "industry 4.0". Big Data analysis is extensively used in the HR field on various levels (hiring process, talent management, etc.).

it is evident that In case Big Data include identifiable personal information, all Big Data analysts must comply with the rules set in the EU Data Protection Law.

Big Data processing within the scope of the new EU Data Protection Regulation

As of May 2018, pursuant to the introduction of the EU Regulation 2016/679, also known as the "General Data Protection Legislation" (the GDPR), all European Union members shall constitute one single data protection territory where the same legal provisions will apply.

Pros

The GDPR offers a clear detailed regulatory framework for all establishments handling data ("data controllers"/"data processors"). Such framework is now less complicated, since notifications to the Data Protection Authority will be, as of May 2018, abolished, significantly reducing thus bureaucracy.

Moreover, data subjects rights' are being strengthened (right to information, access, rectification, erasure, data portability and objection) increasing in such a way the protection of same against eventual violations by companies established within the EU as well as ensuring a free movement of personal data within the internal market.

The GDPR also enables companies to invest on privacy by design techniques,

such as encryption, anonymization, pseudonymization, and data minimization, making them active stakeholders on devising and implementing data protection practices.

Cons

Big Data may initially not contain personal data, but it is not unlikely that their analysis may create personal data. As Big Data is being characterized by the four *Vs* (i.e. Value, Velocity, Variety and Veracity), data controllers and big data analysts are expected to be fully compliant with the EU Data Protection Law at all times.

Under the GDPR, companies not established in the EU shall still have to abide by the rules of EU Data Protection Law, in cases where the data subjects are residing in the EU. As a consequence, third-country companies face the challenge to identify, within the vast volume of Big Data, the personal data belonging to EU citizens and ensure their lawful processing.

Moreover, in case of such further processing Big Data analytics may encounter limitations set by the purpose for which said data has been collected. Companies performing further processing of Big Data must be able to prove that the new purpose of processing is still fair, lawful and compatible to the original one. Such caution should be exercised in cases where Big Data analysis may lead to profiling and automated decision making.

Finally, those who fail to meet the GDPR's rules and provisions face the risk of imposition of severe administrative fines which may entail a serious financial impact to a Company's operation.

Practical guidelines for Companies handling Big Data

- Enhance transparency; draft clear and comprehensible privacy policies and ensure that they are easily accessible by the data subjects concerned,
- Consider appointing a Data Protection Officer and provide his contact details to the data subjects and the local regulatory authority,
- Consider conducting a Data Protection Impact Assessment; such assessment is a legal obligation in case the processing of data is likely to result in a high risk to the rights and freedoms of data subjects,
- Develop privacy by design techniques.
- Do not be complacent; always monitor: **i)** whether your Big Data include or is likely to produce personal data**, ii)** whether the purpose of further processing is still lawful and compatible to the original one. In case the purpose of further processing is not compatible obtain data subjects' consent.

KYRIAKIDES GEORGOPOULOS
Law Firm

Contact

For any further comment or query, please contact the KG lawyer you are in contact with or the Data Protection practice team.

Effie G. Mitsopoulou (Partner)
E-mail: e.mitsopoulou@kglawfirm.gr (Athens office)
Ersi Michailidou
Email: e.michailidou@kglawfirm.gr
Theodoros Giannakopoulos
Email: t.giannakopoulos@kglawfirm.gr
Panagiota Tsinouli
Email: p.tsinouli@kglawfirm.gr

Main (Athens) Offices
28, Dimitriou Soutsou str.,
115 21, Athens
Greece
Tel: +30 210 8171500
Fax:+30 210 68 56 657/8

Thessaloniki Branch
17, Ethnikis Antistaseos
551 34 Thessaloniki
Greece
Tel: +30 2310 441552

www.kglawfirm.gr