A NEW LAW ADOPTED IN THE IMPLEMENTATION OF THE GDPR IN ROMANIA

A new law will enter into force as of 31 July 2018 as a new instrument in the implementation of the Regulation (EU) no. 2016/679 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (the "**GDPR**") in Romania.

Law no 190/2018 ("**Law no. 190/2018**") brings some more rules on processing of special data, as well as some exemptions from these rules for certain categories of data processing.

INCREASED GUARANTEES FOR PROCESSING OF SPECIAL CATEGORIES OF DATA

Processing of health data

As of 31 July 2018, processing of genetic, biometric or health data may only take place with the explicit consent of the data subject or when this is required by an express legal provision. For now, the law seems to leave no room for processing of such data for a legitimate interest of a business.

Processing of national identification numbers

Any processing of a national identification number for a controller's legitimate interest may be undertaken only subject to certain guarantees amongst which the mandatory appointment of a Data Protection Officer ("**DPO**"). This applies to any situation in which documents containing such identification numbers are collected or used by a data controller/processor. These more restrictive rules should seriously limit the situations in which private entities process personal identification numbers for reasons based on legitimate interest. It is expected that many companies will rethink various processes where they used to rely on using ID cards of individuals with whom they are in contact.

On the other hand, it is not very clear how public authorities will apply these restrictions, since the highest use of national identification details occurs when dealing with public authorities. However, the same Law 190/2018 also ensures a buffer for the authorities or public bodies failing to become compliant with these new rules in due time, by regulating a milder sanctioning regime, as further detailed below.

Key aspects

- limitation of processing genetic and biometric data for reaching automatic decisions or for profiling purposes
- limitation of processing national identification numbers for legitimate interests
- reinforcing the conditions for monitoring means used by employers regarding their employees
- derogations from the GDPR for data processing for academic, scientific, research or journalistic purposes
- specific derogations from the GDPR for political parties, national minority organizations and NGOs
- regulation of national accreditation rules for certification bodies
- limitation of sanctions for public authorities and a staggered approach in case of identification of breaches
- change to the Law 102/2005, regarding the functioning of the Data Protection Authority, as amended through Law no. 129/2018, for the repealing of legal provisions regulating the maximum term for applying sanctions for breaching the GDPR

Processing of data in the context of monitoring of employees

The rules previously imposed by specific decisions or practice of the Data Protection Authority regarding the processing of data by means of monitoring of employees, either in terms of monitoring electronic correspondence or by video surveillance, have now become law.

Prior to implementing any monitoring measures in the workplace, the employer must make sure that other less intrusive methods have been tested and have not proven to be efficient. This should mean an actual and documented attempt from the employer. Also, employees' representatives or unions must be consulted and the duration for which information may be stored cannot be longer than 30 days.

This last requirement regarding the retention term for the data resulted from monitoring an employees' correspondence or from video surveillance should be carefully considered when planning for investigations or other actions that may involve monitoring of employees. Based on a proper justification, the 30 days term may be extended; this will however need to be documented in advance.

CERTIFICATION BODIES

Law 190/2018 empowers the Romanian Certification Association (RENAR) to set the requirements, together with the Romanian Data Protection Authority, for the certification of the various services providers who intend to offer certification of DPOs as per the GDPR. RENAR will also be the national body to oversee the certification services market.

SANCTIONS

Law 190/2018 also enters further details on how sanctions regulated by the GDPR apply.

One of the most important rules set is that public authorities and bodies found in breach of the GDPR requirements will first be warned and a remedy plan will be imposed by the Data Protection Authority. Only after failing to fulfil the measures set in the remedy plan, pecuniary sanctions may be applied. Fines in this case are capped at maximum RON 200,000 (approx. EUR 43,245).

In case of private entities or individuals on the other hand, there is no such protective view. These may be sanctioned directly with a fine, depending on the seriousness and the consequences of the breach. No intermediary levels are set for the fines applicable to private entities/individuals. These will be computed within the limits set by the GDPR.

In addition, Law 190/2018 repeals the 3 years statute of limitation applicable to data protection breaches that was set up by Law 129/2018 earlier in June. This means that statute of limitation will need to be further established based on the general rules of civil law.

CLIFFORD
CHANCE
BADEA

CONTACTS

Nadia Badea
Partner

T +40 21 6666 102
E nadia.badea
@cliffordchance.com

Ecaterina Burlacu
Senior Associate

T +40 21 6666 144
E ecaterina.burlacu
@cliffordchance.com

www.cliffordchance.com

Clifford Chance Badea SPRL, Excelsior Center, 28-30 Academiei Street, 12th Floor, Sector 1, Bucharest, 010016, Romania