8 March 2012

Our ref.: 243976

BILL TO REFORM THE EU'S RULES ON THE PROTECTION OF PERSONAL DATA

Introduction

25 January 2012, the Commission proposed a major reform of the rules on the protection of personal data. The aim of EU's rules on the protection of personal data is to protect physical person's basic rights and freedoms, as well as to ensure a free exchange of data within the EU.

The Commission's bill updates and modernises the principles laid down in the existing directive on the protection of personal data from 1995 (95/46/EC), and seeks to take into account the technological development where the extent of data sharing and data gathering has increased significantly.

The material amendments in brief

The material amendments are:

- Companies with more than 250 employees must hire a data protection officer (DPO)
- Companies have a duty to notify the authorities as well as the people affected by a breach of the personal data security
- The fine cap is raised to 2% of a company's global turnover if the personal data rules are violated

The bill has not yet been passed, but the amendments will in all likelihood be passed within a few years, and companies should take the proposed amendments into account

in relation to the companies IT systems and procedures concerning the handling of personal data.

The bill in detail

The bill's most important amendments compared to the existing rules are briefly described here:

Specification of the geographical scope of application

Controllers established in countries outside the EU are already subject to the directive on the protection of data. The Commission's proposal defines when a controller established outside the EU is subject to the directive. A controller is subject to the directive if its activities are related to a) the offering of goods and services to EU-individuals or to b) the monitoring of EU citizens' behaviour.

Particularly, the purpose is to extend the span of the directive to include Facebook and other similar foreign services.

Finally, the bill applies directly, contrary to the directive on the protection of personal data, in the individual EU member states, and therefore does not need to be implemented nationally, thereby ensuring uniformity. Possibly, it has been a problem that the directive on the protection of personal data from 1995 was implemented differently in the individual member states.

Strengthening of the registered person's rights

Article 17 of the bill introduces a "right to be forgotten". This is the right to have data stored either at the data controller or on the internet deleted.

Furthermore, a registered person must have the opportunity to move his/her own personal data from one online service to another, e.g. between Facebook, Google+ and Twitter (i.e. a right to data portability in Article 18 of the bill).

Finally, the registered persons must be allowed access, by the data controller, to a copy of the information which is being processed, in an ordinary electronically and structured format which the person registered may use at a later point in time.

Duty of notification when the personal data security is breached

Furthermore, Article 31 imposes a duty to notify the supervising authority when the personal data security is breached. This is already in force in the telecommunications sector, where the Danish Business Authority (formerly the IT and Telecom Agency) must be notified. The duty of notification laid down in Article 31 is based on the notification of breaches of the security on personal data in Article 4(3) in the e- data protection

directive. The notification must be given without undue delay, and if possible within 24 hours after the data controller was made aware of the breach of the personal data security.

Finally, according to Article 32 of the bill, registered persons must be informed of the security breach if the protection of personal data or privacy is at risk of being offended. For instance in case of a hacker attack on an IT-system, where personally sensitive data has been damaged or compromised.

Tightened requirements to consent
Equally, the bill imposes tightened requirements to the consent of a registered person, meaning that the consent will no longer be applicable as a basis for handling if there is a significant imbalance between the registered person and the data controller, e.g. if there is state of dependence between them. This would especially be the case, when dealing with consents given in an employment relationship.

In regard to the personal data of persons aged 13 and under, consent must be obtained from the child's parents or legal guardian in connection with offers about information society services.

Pursuant to Article 7, consent must be given expressively, and it is assumed that it is not adequate that the consent is given in connection with general terms and conditions as a consent must be clearly separated from any other text or other conditions (explicit opt-in consent).

Tightening of the controller's responsibility and increased self-regulation
The controller will be obliged to limit his/her handling of personal data to an absolute minimum and must in that regard comply with the proportionality principle, in that handling may only take place if the purpose cannot be achieved through less extensive means.

Equally, companies are required to compose and implement procedures for the handling of personal data. Companies with more than 250 employees have a duty to hire a data protection officer (DPO) in order to ensure that the company comply with the rules in the directive.

Companies which wish to transfer data to third world countries which do not offer the same level of protection as within the EU will have the opportunity, given certain conditions, to transfer data to these countries if the transfer is necessary based on legitimate interests, e.g. in group affairs or through outsourcing to data processing units, e.g. cloud-solutions. In that regard, groups of companies must be allowed easier access to

impose the so called "Binding Corporate Rules" which regulate the transfer between companies in a group. Among other things, these will in future only need approval by the authorities in one EU country.

Tightening of the fine level
The bill will impose significantly larger fines for breaches of the personal data rules. The fine level from now on is to be between EUR 250.000 and EUR 1.000.000, depending on the type of breach.

Alternatively, when dealing with companies, depending on the type of breach, the company may be charged with fines of up to 2 % of its total annual global turnover if the personal date rules are breached. Article 79 of the bill lists and classifies the severity of a number of certain breaches e.g. mistakenly charging fees for information to the registered person, inadequate update of information, lacking delivery/transfer of the registered person's information, lacking or late notification of breach of personal data security, lacking appointment of data protection officer, unjustified transfer of personal data to a third world country etc..

The fine cap is up to 1% of the company's annual global turnover if the company for instance breaches the rules regarding collection of information. The fine cap of up to 2% applies if the company's breach is more severe, for instance the handling of information without warrant or consent from the registered person.

Consequences for the existing treatment of personal data
If the bill is accepted in its present shape, the changes will impose far-reaching obligations for business owners when they treat personal data information, and considerably larger sanction may be incurred. By this, personal data is raised op to the management level and is no longer just a part of general compliance.

According to the Commission, the purpose of such obligations is to cater for the European citizens and businesses. Instead of 27 national statutes, which at the moment is the case, there will only be one statute (i.e. the regulation) and only one supervisory authority which regulates all matters. This is to relieve the businesses from administrative burdens when exchanging information, while they on the other hand are subject to stricter obligations when treating the information. For the citizens, this ensures that there are uniform rights for all EU citizens.

Users of social networks and the like will have the possibility to have their data completely removed, e.g. when they close an account. New and more extensive regulation has been necessary for a while, as the present regulation was passed 17 years ago.

The Commission's bill does not regulate what is meant by "the right to be forgotten" in relation to journalistic or historical information.

The next step

The bill from the Commission is now forwarded to the European Parliament and the Council of Ministers for debate, and it is presumed that this will result in changes to the bill. If the bill is passed, it is planned that the regulation will come into force two years after final adoption.

Within the next couple of years, it is presumed that the bill, in a revised version, will be passed based on the above mentioned general points. 2012 will presumably become a decisive year for businesses and other participants to affect the bill.

Businesses should already now begin to consider the contents of the bill with reference to their different systems and processes for treating personal data, for example when they purchase and structure their IT systems and when they organize their administrative processes, as a rearrangement of the businesses systems and processes with regard to the new rules cannot be made from one day to the other.

If you have any questions or require additional information on the above, please contact Partner, Nicolai Hesgaard (nhe@mwblaw.dk), Attorney Henrik Syskind Pedersen (hsp@mwblaw.dk) or Junior Associate Maria Thomsen (mth@mwblaw.dk)
The above does not constitute legal counseling and Moalem Weitemeyer Bendtsen does not warrant the accuracy of the information.

With the above text, Moalem Weitemeyer Bendtsen has not assumed responsibility of any kind as a consequence aft a reader's use of the above as a basis decisions or considerations.