February 2015

NEW EU DATA PROTECTION RULES KNOCKING ON THE DOOR

"*This reform is a necessity, and now it is irreversible. Europe's directly elected parliamentarians have listened to European citizens and European businesses and, with this vote, have made clear that we need a uniform and strong European data protection law, which will make life easier for business and strengthen the protection of our citizens*" - said Vice-President Viviane Reding, the EU's Justice Commissioner.

Although not as fast as desired, the European Union (EU) data protection reform is moving forward. In year 2012 the European Commission suggested an overall update of the 1995 Data Protection Directive and made two legislative proposals: a Regulation, setting out a general EU framework for data protection, and a Directive for the purposes of criminal investigations. On 12 March 2014, the EU Parliament approved the draft Regulation and the draft Directive. For the proposed legislative acts to become law, they have to be adopted by the Council of Ministers using the "ordinary legislative procedure" (co-decision). In June 2014, the Council agreed on a general approach only on specific issues and provisions of the draft Regulation (mainly on the provisions in Chapter V "Transfer of personal data to third countries and international organizations"). However, the Presidency of the Council expressly indicated that "noting is agreed until everything is agreed". Currently discussions within the Council proceed with full speed and the next meeting is scheduled in the beginning of October 2014. It is everyone's expectation (and aim) to have the adoption procedures finalized by the end of this year.

This article aims to provide a brief overview of the main amendments to be introduced in the European data protection legislation. It describes the amendments and their potential effect from the data controllers' point of view, as they are eventually the ones that will face the challenges of the new rules once they are introduced.

The reasons behind

Indeed, trust in the efficiency of data protection rights has been significantly affected by some recent cases. It all started when the Snowden affair in 2011[1] opened questions on whether people's personal data is secured in the digital environment and how to protect the EU citizens' data outside the EU. Later in 2011, an Austrian law student – Max Schrems, started a debate about Facebook users' personal data after discovering that the social network kept a file of 1,224 pages of information about him, most of which he considered 'deleted'[2]. Further, in 2013 the technology giant Sony Computer

[1] Former U.S. intelligence contractor, Edward Snow-den, leaked details of U.S. surveillance programs for monitoring vast quantities of emails and phone records worldwide

[2] The 24-years old law student was shocked by the enormous amount of data Facebook was keeping about him (all people that he friended and de-friended, pages he ever liked, pocked, commented, and even deleted from his profile). Apparently, he discovered that Facebook' headquarter was in Ireland (i.e. in EU), and filed 22 claims against Facebook

Entertainment Europe was fined for having allowed two major data protection leaks 2011[3] and was late in discovering that the leaks actually took place.

These and many more cases within the EU found their reflection in the proposed reform provisions – i.e. the Snowden case led to reconciliation of the 'Safe Harbor' system, Facebook grounded the development of "the right to be forgotten", and the technology companies' data leaks increased the level to data security notification requirements imposed on the data controllers.

What should data controllers know about the new regime?

a. From a single Directive to a Pan-European law

As the European Commission noted[4], although the Data Protection Directive[5] served its purpose to establish the main data protection principles across the EU, it was (having the force of a 'directive') incoherently implemented in the national legislations of the member-states. This led to an administrative and a legal uncertainty for the data controllers operating in multiple jurisdictions in the EU[6]. Therefore, the new reform package of the European Commission took the form of a regulation – i.e. one law, directly applicable in all member states and their Data Protection Authorities ('DPAs').

b. EU and non-EU data controllers captured by the Regulation

One of the main changes introduced with the new Regulation is the wider territorial scope of its application. It is the aim of the European Commission to also encompass non-EU data controllers (e.g. global multinational companies) and oblige them, to comply with the EU data protection regulations, should they wish to have access to the European market and the European consumers.

The new Regulation is expected to cover:

- EU data controllers, no matter where the personal data is being processed; and
- Non-EU data controllers if they process personal data of EU citizens for the purposes of:

---

before the Irish Data Protection Commissioner. The case become famous under the name "Europe v Facebook"- http://europe-v-facebook.org/

3 Sony discovered a nearly 25m customers' details from its Sony Online Entertainment' network stolen and another 77m – from its PlayStation Network

[4] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union", Brussels, 4.11.2010, COM(2010) 609 (final)

[5] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[6] For example, the different Member states developed different approach to the notification requirements imposed on the data controllers – some have generally exempted small/medium data controllers (the exact definition also varies) while others, tied the notification requirements with the significance of the personal data processed (i.e. sensitive data)

- offering of goods or services to that data subjects[7];
- monitoring of their behavior.

This scope of the Regulation was broadly supported by both the European Parliament (EP) and the Council[8]. The Council's position only differs from the EP's as to the exact scope of the monitoring of the behavior of data subjects. The Council suggested that the Regulation's rules only apply if the data controller monitors behavior within the EU, where the EP propose the rules to apply to any sort of monitoring of data subjects, not only to the monitoring of behavior. The compromise is yet to be decided.

c. *SME – looser regulations and available exemptions*

Despite the tendencies of strengthening the data protection regulations, a flexible approach is adopted with regards to small and medium enterprises ('SME'), the underlying idea being that "... the baker on the corner will not be subject to the same obligations as a (multinational) data processing specialist"[9]. SMEs are allowed the following, among others, exemptions from the data controller's regime: they are not required to appoint a Data Privacy Officers (see p. 'f' below); they are exempted from all notifications to the DPAs; they may charge a fee for providing a data access of the data subjects; they are not required to conduct an impact risk assessment on the personal data, etc.

d. *"One stop shop"*

A major change envisaged by the new Regulation and targeted at the formation of 'one continent-one law' system (see p. 'a' above) is the role of one centralized 'leading' DPA competent to supervise the separate data controllers (and data processors). The leading DPA is to be determined by the member state of the main establishment of the data controller. This 'one stop shop' approach will ease the administrative burden of the data controllers having to comply with 28 different DPAs. However, it may also cause a number of logistics discrepancies between the DPAs which could only be overcome by a strong cooperation between them.

Member States have already expressed their concerns regarding the practical efficiency of the approach, in particular - the enforceability of the leading DPA' decisions in other member-states where the data controller is present (apart from its main establishment). To overcome the different opinions, the Council outlined the main issues on "one stop shop" mechanic[10] to be further discussed, assumingly on the next Council's meeting in

[7] The European Parliament went even further by suggesting that in order for a non-EU data control-ler/processor to fall in the scope of option (a) no regard will be given whether the goods/services were offered against payment– current art. 3 of the draft Regulation

[8] The Council reached partial general approach the text of Article 3(2) (territorial scope), the text concerning the respective definitions of "binding corporate rules" and "international organizations" (Articles 4(17) and (21)), and the transfer of personal data to third countries or international organizations (Chapter V) of the draft regulation. The full text of the agreement could be seen here http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT

[9] "Progress on EU data protection reform now irreversible following European Parliament Vote", Memo, Strasbourg, 12 March, 2014, European Commission

[10] The content of the orientation debate on the one-stop shop could be found here:

October 2014.

e. *Data processors – obligations as data controllers*

The draft Regulation provides a detailed guidance of the data processors' functions and obligations[11]. Requirements as to the content of the act (contract or other written act) that regulates the relationship between the data controller and the data processor, imposes in many aspects the same level of care and obligations to the data processor as those of the data controller[12] (e.g. in terms of security requirements, notification obligations upon breach, documentation of all processing operations, cooperation with the data protection authorities).

f. *Data Privacy Officer – the employee in charge*

Aimed at ensuring a more stringent supervision, the draft Regulation includes mandatory appointment of a Data Privacy Officer ('DPO')[13] for public authorities and bodies, large data controllers (undertakings with more than 250 employees), and data controllers which main subject of activity involves data processing. The DPO is the employee designated to be the 'compliance person' in the data controller's enterprise, responsible for the data processing security and the communication with data subjects.

g. *No delay to notify data breaches*

The draft Regulation obliges data controllers to notify data breaches to the DPAs without undue delay and where feasible not later than 24 hours after having become aware of it.

h. *Extended rights of the data subjects*

With respect to data subjects, the new rules aim to make the exercise of data protection rights easier and more effective, as well as to create a feeling that people are 'in control' of their personal data. Recent researches have shown that just over a quarter of social network users, and even fewer online shoppers, feel safe of their personal data. However, granting broader rights to data subjects always has a twofold effect, as it inevitably result in additional obligations for the data controllers such as:

- Explicit Consent

  Consent is the most common 'legitimate' ground used by data controllers for processing of personal data. The requirement for an 'explicit' consent means that either 'a statement' or a 'clear affirmative action' should be expressed by the data

---

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010139%202014%20INIT

[11] Art. 26, para 2 of the draft Regulation set forth the main obligation imposed on data processors

[12] For details, see art. 26 – 35 of the draft Regulation

[13] A DPO is a designated employee responsible for the data processing' security measures within the enterprise as well as entrusted with the communication with data subjects, including where "explicit consent" needs to be implemented

subject. This requirement, although broad enough to allow different mechanics for provision of consent, would request a conduct on the side of the data subject, '... including by ticking a box when visiting an Internet website'. Silence or absence of any action/conduct will not be deemed a valid consent, thereby forcing a number of online services providers to change their current user's data processing mechanics.

- Special rules for children

  The Regulation sets forth a special data protection definition for children[14]. Further, a more stringent care is prescribed in cases where children below the age of 13 are directly offered an information society service. In these cases the data processing consent shall be either given by the child' parents or authorized by them.

- The right to be forgotten

  The essence of this new concept/right[15] is to enable data subjects to withdraw their consent at any time and request full deletion of their personal data (including where the information is stored by social networks, cloud computing platforms or search engines). A data controller may override such request only by evidencing a 'legitimate interest'.

- Data portability - transfers from one service provider to other

  The EU Commission noted that certain services depend on a specific platform, allowing a limited possibility for individuals to move their data when changing the service provider. The right to data portability entitles individuals to withdraw their personal data (including, photos, friends' lists, messages) and transfer them to another service provider, as far as this is technically feasible.

i. Jurisdiction on disputes

New rules significantly evolve the individuals' right to lodge a complaint by providing them a possibility to choose a jurisdiction[16]. In practical terms, this means that although another DPA may be the leading DPA with respect to certain data controller (see p. 'd'), 'individuals will always be able to go to their local data protection authority'. The aim is to improve the current system in which individuals residing in one Member State have to file complain in another Member States, following the establishment of the data controller.

j. Privacy by design/privacy by default

Privacy by design and by default principles request from data controllers to organize

[14] Under p. (18) of art. 4 of the draft Regulation de-fine a child as a person under the age 18. Until now the EU data protection rules did not contain a legal definition or a separate regime for children

[15] The European Court of Justice already outrun the draft-Regulation and developed a case law on the 'right to be forgotten' earlier this year by requiring Google and other Internet search engines to remove "inaccurate, inadequate, irrelevant or no longer relevant" information from their search results at the request of users

[16] Art. 73 of the draft Regulation

upfront their structure, technology and procedures in a way that will ensure compliance with the rights of the data subjects in terms of consent, information, access and necessity of processing[17].

Implications to emphasize

Implications stemming from the new Regulation are already 'red flagged' – concerned data controllers/processors, including non-EU data controllers/processors, will need to invest time and resources to ensure that appropriate internal policies and procedures are implemented to face the higher data processing requirements. Minding the serious sanctions planned by the EU authorities, these are not matters to stay out of an enterprise's budget.

a. Administrative and technical burdens

Compliance with the new data protection requirements will force both EU and non-EU data controllers to adopt new internal compliance policies (codes of conduct)[18] and mechanics for implementing the higher standards. Documentation evidencing all processing operations of the data controller/processor, managing of the 'explicit' consent requirement, complying with security levels, technical measures to enforce 'the right to be forgotten', etc. – it sounds like a whole new organizational structure for the data controllers to build and daily operate.

b. New employee' position

With the introduction of the obligation of a DPO, many data controllers will have to be prepared for an additional salary. The role of the DPO involves the performance of many tasks from administrative, legal and technical nature and would require an additional full-time position.

c. Upfront compliance

Additional costs will be borne by a data controller to comply with the new principles for privacy of design/ privacy by default and consider in advance what legal, organizational and technology procedures should be put in place, for its activity to comply with the data protection rules.

d. Sanctions not to underestimate

The non-compliance with the obligations in the Regulation might trigger the imposition of a fine, up to 5% of the annual revenue. "The EU wants to send a message to the whole world: You now need to take data protection seriously if you want to do business in Europe". However, there are ongoing concerns for the disproportionality of such sanctions and whether they might discourage more than encourage data controllers (especially

[17] Art. 23 of the draft Regulation

[18] See Art. 38 of the draft Regulation for the mandatory minimum content of the codes of conduct.

non-EU) giving priority to the personal data safety. Another still pending question is on the proper calculation of these sanctions.

About Wolf Theiss

Wolf Theiss is one of the leading law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We have built our reputation on a combination of unrivalled local knowledge and strong international capability. We opened our first office in Vienna over 50 years ago.

Our team now brings together over 350 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region. For information about our services, please contact:

Anna Rizova
Managing Partner
anna.rizova@wolftheiss.com
T +359 86 13 700

Hristina Dzhevlekova
Associate, Attorney-at-law
hristina.dzhevlekova@wolftheiss.com
M +359 888 101 652