REDA 2015

THE REFORM OF PERSONAL DATA PROTECTION: WHAT PERSPECTIVE?

In 1981, the Council of Europe opened for signature Convention 108 for the protection of individuals with regard to automatic processing of personal data. This was the first international legal instrument for the protection of personal data, which laid down the principles for processing such data. Convention 108 and its Protocols have been signed and ratified by the Republic of Cyprus. This legislative tool proved quite useful and it was the founding building stone for Directive 95/46/EC, adopted by the European Union in 1995. The Directive was transposed into the Cyprus legal order by the Processing of Personal Data (Protection of Individuals) Law of 2001. Globalization, technological developments, particularly in the fields of internet and communications and over-growing trans-border flows of data called for the need for revising these legal instruments.

A text for the modernization of Convention 108 is currently pending before the Committee of Ministers of the Council of Europe, expected to be finalized and adopted within 2016. At the same time, the European Commission is negotiating with the
Co-Legislators, the Council and the Parliament, a package of 2 reform Proposals, a Regulation and a Directive, which will establish the new data protection legal regime in the Union. These proposals are currently at the stage of trialogue. The Council of Europe (CoE) and the European Union (EU) recognize the imperative need of adopting compatible legal instruments, taking into account recent milestone rulings of the European Court of Human Rights (ECHR) and the Court of Justice of the EU (CJEU), respectively.

What does this reform aim for? This is what this panel is about to address.

It has been said, that personal data are the hard currency of the 21st century. A lot of services are offered to us on-line free of charge but, at the cost of intruding our privacy. The new legal regimes, both at the CoE and at the EU should, firstly, aim to strengthen citizens' rights, who should be properly informed about the processing of the personal data, before they consent to it. Secondly, due to rapid technological developments and innovations, it is important that the data protection reform remains technologically neutral, so that it withstands the test of time. Thirdly, it should provide a robust and harmonized regime for facilitating international data flows, with respect to the fundamental rights of European citizens. These are only few of the challenges that the legislators have to meet during the endeavor of the reform.

I will now give the floor to our esteemed colleagues, who will further elaborate on this issue.

05/11/2015

Milestone CJEU rulings:

1. The Annulment of the Retention Directive 2006/24/EC

Joint cases: Requests for preliminary rulings by the High Court of Ireland in Digital Rights Ireland Ltd case C-293/12 and by the German Constitutional Court C-594/12

Internet and telephone service providers operating in more than one Member States were subject to different obligations, imposed by national Laws, as regards the retention of communication data for billing purposes. The Directive aimed to harmonize these different retention obligations for a period of 6-24 months. At the same time, it provided that law enforcement authorities can access these data, if this is laid down by national Law. The CJEU ruled that the Directive entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary. In its judgment, the CJEU made reference to ECHR case Law.

In Cyprus, Directive 2006/24/EC was transposed into national legislation by Law 183(I)/2007. In 2013, the Cyprus Supreme Court, in a case brought before it, ruled that the annulment of the Directive does not affect the national Law 183(I)/2007, which remains into effect.

2. The Google Spain Case C-131/12

An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties. Thus, if, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results.

The right to be forgotten is enshrined in Article 17 of the Proposal for a General Data Protection Regulation (GDPR) which will replace Directive 95/46/EC. The GDPR is currently at the stage of trialogue. The right to be forgotten is not a novel right, but rather an extension of the right for erasure provided for by Directive 95/46/EC, which is strengthened by the GDPR. The right for de-listing established by the CJEU in the Google Spain (Costeja) Case proves that there is at least one effective technical solution for exercising the right to be forgotten but it should not be seen as the only way for exercising the right to be forgotten.

3. The Safe Harbor Case

Request for preliminary ruling by the High Court of Ireland in the case of Maximillian Schrems vs Data Protection Commissioner C-362/14

The CJEU invalided the Safe Harbor Decision 2000/520/EC. US intelligence services' access, on a generalized basis, to all the personal data of all the persons whose data is transferred from the EU to the US without any differentiation, limitation or exception being made, compromises the essence of the fundamental right to respect for private life. Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data

relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection. The Commission did not have competence to restrict the national supervisory authorities' power to challenge an adequacy Decision. The Irish Commissioner has to examine Mr Schrems' complaint with all due diligence and effectively decide if, transfers of the data of Facebook Ireland to the US should be suspended on the ground that that the US does not afford an adequate level of protection.

Key reforms under the GDPR:

The one stop shop

Every organization and every citizen may bring their cases before one DPA, on the basis of various criteria such as the MS of the establishment of the controller, or the MS of residence of the data subject. Where required, in cross border cases, the DPA of the MS where the controller has his Main Establishment, shall act as Lead Authority.

Note: Article 4(1)(a) (Applicable Law) of Directive 95/46/EC provides that the provisions of the Directive apply to the processing of personal data carried out *in the context of the activities of an establishment of the controller* on the territory of the MS; when the same controller is established on the territory of several MS, he must take necessary measures to ensure that each of these establishments complies with the obligations laid down by the applicable national law.

Directive 95/46/EC did not provide a definition of "an establishment of a controller". The GDPR provides definitions both for the "establishment" and the "main establishment" of the controller.

The European Data Protection Board EDPB

The Art.29WP consultive body will be replaced by the EDPB, which will have a legal entity and it will issue binding decisions. In certain occasions, the EDPB may take up cross border cases, on merits of the impact of each case and the number of EU citizens affected. The EDPB will act as the last resort in cases where DPAs cannot resolve cross-border cases in the frame of the consistency mechanism. The EDPB's decision will have binding effect on DPAs.

The Consistency Mechanism

It will be activated in cross-border cases as a tool for resolving DPA's differences on the handling of such cases. It aims to provide a harmonized approach and a remedy for the problems stemming from the fragmentation of Directive 95/46/EC.

The right to be forgotten (GDPR Art. 17)

It is not a novel right, but rather an extension of the right to erasure provided for by Directive 95/46/EC, strengthened by the GDPR. The right to de-listing enshrined in the Google Spain (Costeja) CJEU ruling proves that there is at least one effective technical solution for exercising the right to be forgotten but it should not be seen as the only way.

The right to data portability (GDPR Art. 18)

When data are processed electronically, data subjects have the right to ask copies of their personal data in commonly available electronic forms, for further use and or for passing them to other controllers of their choice.

Accountability

The GDPR aims to reduce costly red tape burdens by promoting self regulation. At the same time, it establishes the principle of Accountability, which obliges Controllers and Processors to demonstrate their compliance with the GDPR.

Privacy by design

Technical privacy safeguards should be embedded in software and hardware solutions, at the stage of manufacturing/ designing.

Privacy by default

Software and hardware solutions should provide to users, privacy friendly settings by default.

Privacy Impact Assessments PIAs

The GDPR defines the cases where controllers are obliged to carry out PIAs before implementing measures that restrict the rights to privacy and data protection.

Data Protection Officer DPO

DPOs were optional under the Directive. The GDPR defines the cases where DPOs should be mandatory and provides some exceptions for SMEs.

Data Breach Notification

Under the e-privacy Directive 2002/58/EC, the obligation to notify data breaches, to DPAs and or to data subjects, was constrained only to communication service providers. The GDPR extends this obligation to all controllers.

Abolition of notifications and prior authorizations

The GDPR aims to reduce costly red tape burdens by promoting self regulation. Controllers are no longer obliged to submit notifications to DPAs and prior authorizations are limited only to transfers. DPAs will carry out inspections ex ante rather than ex post.

Key reforms under the Proposal for a Directive:

It replaces Framework Decision 2008/977/JHA which applies only to data exchanged among MS's competent law enforcement authorities and to the onward transfers of such data to third countries, for purposes of prevention, investigation, detection and prosecution of serious crime and terrorism. The Directive applies the data protection principles to the processing of personal data carried out by law enforcement authorities at national level to data exchanged among MS's competent law enforcement authorities and to the onward transfers of such data to third countries.