diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 07/04/2016

All'indirizzo http://www.diritto.it/docs/38074-european-general-data-protection-regulation-territorial-scope-at-a-glance

Autori: Marcoccio Gloria , Luciano Delli Veneri

European General Data Protection Regulation - Territorial Scope at a glance

European General Data Protection Regulation - Territorial Scope at a glance

Gloria Marcoccio - gloria.marcoccio@glory.it, Luciano Delli Veneri - luciano.delliveneri@gmail.com

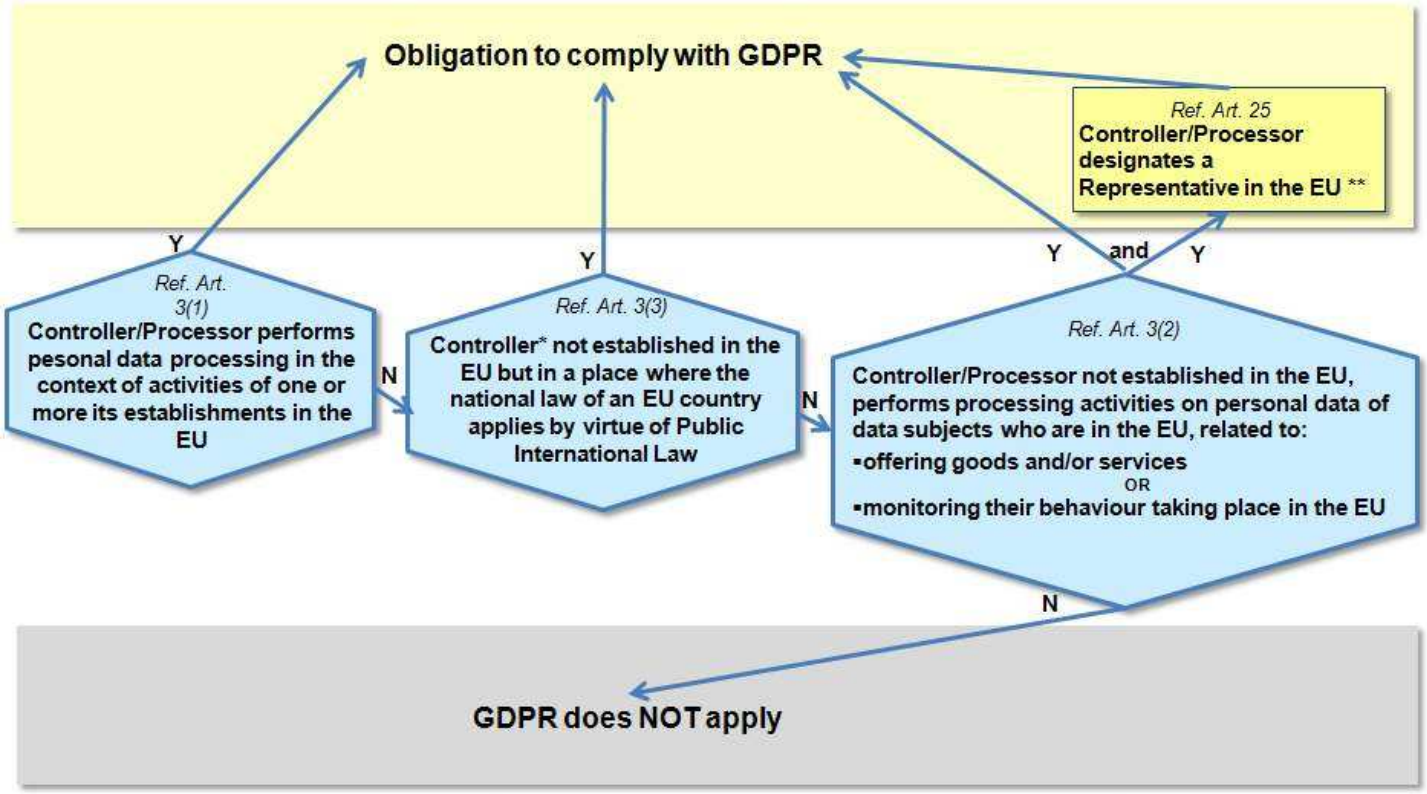
April 4, 2016

Introduction

One of the essential news brought by the European General Data Protection Regulation[1] (GDPR) is represented by its broad territorial scope (Article 3) not limited to the 28 EU Member States: as a result a very wide variety of enterprises, companies and, in general, organizations located everywhere in the world and whatever is their business are required to comply with the GDPR provisions if such business is targeted to the EU how determined by the GDPR.

The flow chart in Figure 1 summarizes the essential decision points which determine the boundaries of the GDPR Territorial Scope.

Figure 1 - Essential decision points to determine the boundaries of the GDPR Territorial Scope



**Maybe a typo in the GDPR text officially available, since it is reasonable that such requirement is addressed both to Controllers and Processors*

*** This obligation does not apply to*

- *processing which is occasional, does not include, on a large scale, processing of special categories of data (sensitive data,…see Article 9(1)) or processing of data relating to criminal convictions and offences, and is unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing [please note: this requires accountable decision by relevant Controller/Processor]*
- *a public authority or body*

[1] The European Data Protection Regulation (GDPR) will replace the present UE Privacy directive 95/46/EC; the Regulation shall be published in the EU Official Journal after its formal approval by the European Parliament in plenary session, expected by Spring 2016, and it will be implemented within two years in all the 28 EU Member States (Directives must be transposed in EU national laws, Regulations are directly applicable in all EU countries). This article makes reference to the text of the Regulation on which it has been reached the agreement documented by the press-release: http://www.consilium.europa.eu/it/press/press-releases/2015/12/18-data-protection/.

- For additional information about the new framework of sanctions provided for by the GDPR: "*An overview about sanctions provided for by the new European Regulation on personal data protection*"

http://www.diritto.it/docs/37782-an-overview-about-sanctions-provided-for-by-the-new-european-regulation-on-personal-data-protection

- For an overview about the Data Breach obligations brought by the GDPR and other relevant EU laws: "*Data Breach notification obligations: summary overview of the current EU/Italy legal framework in light of the European General Data Protection Regulation and Network Information Security Directive*"

http://www.diritto.it/docs/37916-data-breach-notification-obligations-summary-overview-of-the-current-eu-italy-legal-framework-in-light-of-the-european-general-data-protection-regulation-and-network-information-security-directiv

Essential features of the GDPR Territorial Scope

The increased number of not_EU organizations obliged to fulfill the GDPR requirements is mainly based on the following pillars.

1 Both Controllers and Processors are required to comply with the GDPR

In the EU Privacy Directive 95/46/EC (EU Privacy Directive) the Territorial Scope (Article 4) is addressed to the organizations acting in the role of Controllers (they decide purpose and scope of a personal data processing and related security measures), now the GDPR Territorial Scope in addition is addressed also to the Processors (they process personal data on behalf of Controllers).

As an example of typical business activities performed by an organization in the role of Processor, all the companies operating outsourced services, involving EU personal data processing, to an EU or not_EU based legal entity will be required to operate in compliance with the GDPR and as such they will be directly subject to the enforcement actions by the EU Data Protection Authorities (DPA) in case of failures in complying.

Compared with the EU Privacy Directive, the GDPR brings many additional requirements expressly addressed to the Processor, such the Data Breach notification without undue delay to the Controller (article 31), the obligation to maintain specific records of processing activities carried out on behalf of each Controller (article 28), the obligation to designate a Data Protection Officer in some cases (article 35), the specific Processor obligations (article 26 and 27)..., all such requirements involving specific commitment, efforts and costs.

It may happen that many not_ EU organizations could be not fully aware of the law consequences in operating as Processors in the meaning of the GDPR, therefore exposed to the risk of the heavy sanctions provided for by the GDPR (see also the article cited in note 1). In this sense an extensive information campaign should be implemented by the competent authorities in order to increase awareness about GDPR applicability and obligations toward organizations potentially able to provide services in the role of Processor.

2 New wide meaning of EU establishment for business purposes

The original meaning of EU establishment, under the 21 years old EU Privacy Directive (designed and entered in to force well before the 'digital services' era) was inevitability strongly related to the physical establishment of a company within an EU Member State and in consideration of data processing 1) mainly performed in such physical establishment and 2) with regard to data subjects mainly resident in such country.

Along these years the concept of establishment in relation to business purposes of a company has been subject to consistent evolutions driven by the growing availability of the information society and networked services as well as the outsourcing and globalisation trends, moving the focus from the place where a processing occurs to the target toward a business related processing is addressed to. As a consequence the applicable law under the EU Privacy Directive has been analysed in the past by the WP 29[2] with a specific Opinion (Opinion 8/2010 on applicable law- WP179) and in the recent years the European Court of Justice (CJEU) has contributed to extend and clarify the concept of establishment in relation to personal data processing and privacy law applicability with important judgments, among which the most relevant are:

- CJEU judgement of 13 May 2014 in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ('Google Spain')*.
- CJEU judgement of 1 October 2015 in Case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság ('Weltimmo').*

At the end of the last year the WP 29 has consequently updated its 2010 Opinion (Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, adopted on 16 December 2015).

Now, according to the GDPR, "*any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect*". For a company this involves the responsibility to perform an evaluation for taking a decision about the GDPR applicability to its business context in terms of EU establishment.

3 New criterion on GDPR applicability based on offering goods or services

The criterion set out with the EU Privacy Directive in order to determine the applicability of the EU privacy law (the transposition of the EU Privacy Directive in a specific Member State) to a not EU based entity is based on the use by such entity (Controller role only) of means of processing, automated or not, located in a Member State, provided that such means of processing are used not only for transmitting data.

[2] The Article 29 Data Protection Working Party (WP29) was set up under the Directive 95/46/EC, it has advisory status and acts independently, and it is essentially set up with the representative of the 28 EU Data Protection Authorities. With the entry in force of the GDPR the WP29 will be replaced by the European Data Protection Board (EDPB), with increased powers (similar composition of the WP29).

Now the GDPR splits the applicability criterion in two parts (briefly discussed in this Pillar and the next one) and completely redefines the object of the criterion:

'the Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union'.

Therefore the not-EU based organizations need to implement analysis and take decisions in order to ascertain if their cases of business match this criterion for the applicability of the GDPR. A support for taking decision is provided by Recital 20 of the GDPR:

'In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union.'

4 New criterion on GDPR applicability based on behaviour monitoring

The second part of the criterion for applying the GDPR to not_EU based entities:

'the Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union'

Also in this case the organizations need to perform analysis and take decisions about the GDPR applicability at their business, provided that some useful clarifications are provided by Recital 21 of the GDPR:

'The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects as far as their behaviour takes places within the European Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether individuals are tracked on the Internet including potential subsequent use of data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.'

Substantially remained unchanged the EU Privacy Directive provision about the applicability of the European privacy laws when the national law of an EU Member State applies to a not_EU organization by virtue of Public International law.

Some food for thought

Providers of outsourced services such as IT support, HR & payroll services, insurance related services and, the providers of services integrated into the cloud services (i.e. storage systems operators, operation& maintenance managed services,..) whatever is their EU or not_EU establishment, when acting in the role of Processors or Controllers they are required to fulfill the relevant GDPR provisions when processing data in the context of their EU business.

The meaning of the 'data subjects who are in the EU' plays a fundamental role in shaping the effective boundaries of the GDRP applicability for organizations not based in the EU: it is reasonable to do not limit the meaning to the physical location or the places of residence of the individuals and the Controllers/Processors will need to assess other elements such as the language adopted for marketing and selling their goods and services to EU potential customers. About this point it is interesting to bear in mind a CJEU judgment of December 2010 about a case on determining the applicable jurisdiction for selling services by a web site (see the Curia Press Release[3]):

" *In order to determine whether a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Regulation No 44/2001, it should be ascertained whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader's overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with them. The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of*

[3] europa.eu\rapid\press-release_CJE-10-118_en.pdf

expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.

On the other hand, the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled is insufficient. The same is true of mention of an email address and of other contact details, or of use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established. "

From the 'behaviour monitoring' point of view the not_ EU based Controllers/Processors evaluation tasks about GDPR applicability will require their due attention since the meaning of 'behaviour' of an individual is not completely delimited by the Regulation and it can also include geo-location processing activities or other processing for example aimed at safety purposes of for protection of company assets, performed on the personal of workers of an organization, other than the 'typical' case of behaviour monitoring for marketing purposes performed in Internet by means of cookies or device fingerprinting techniques.

Lastly it is important to note that the practical enforceability of the GDPR, against not_EU based Controller/Processor which are to be considered in scope for the GDPR applicability, it appears as a hard task for the 28 DPAs, inter alia it shall require strong coordination among them in order to avoid national based diversities in apply different economical values of administrative sanctions related to a same GDPR obligation which is in force in all the EU Member States: such situation would be unacceptable from several points of view. Furthermore it is noteworthy to underline that for the not_EU based Controllers/Processors in scope for the GDPR, it is provided a specific sanction in case they infringe the GDPR obligation (Article 25) requiring that they designate in writing a Representative in the EU: the fine is up to 10 million euro, in case of undertaking up to 2% of the total worldwide annual turnover, whichever is higher).