ISSN 1127-8579

Pubblicato dal 10/04/2013

All'indirizzo http://www.diritto.it/docs/34905-a-legal-overview-on-the-proposal-of-the-new-regulation-on-data-protection

Autore: Giannini Silvia

A legal overview on the proposal of the new regulation on Data Protection

A legal overview on the proposal of the new regulation on Data Protection

- **Author: Silvia Giannini -**

On 25 January 2012, the Commission published its proposal for a new 'General Data Protection Regulation'. A Regulation is considered the most appropriate legal instrument for avoiding legal fragmentation in each State Members' of the European Union receipt process as it is directly applicable in accordance with the Article 288 TFEU.

The goal of having a Regulation is introducing "a set of harmonized rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market".[1]

This article is aimed to summarize the key changes related to the new data protection approach as reported in the Regulation.

General Provisions

Under this Chapter, the article 4 "Definitions" contains all the definitions set forth in the Directive 95/46/EC as well as some definitions derived from other Directives, such as Directive 2002/58/EC as amended by Directive 2009/136/EC which are related to the 'genetic data', 'data concerning health', 'enterprise', 'binding corporate rules', 'group of undertakings'. The most important one is related to the definition of "data subject's consent" which is defined as "freely, given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed". In this respect, the control should have to bear the burden of proving that the data subject given their consent. Practically, the controller shall keep track of consents received from any customers or data subjects who visited and logged-in their website (please refer to the comment related to article 7 of the proposed Regulation for conditions for consent).

In this respect a point of attention is related to the definition of "data subject": the Regulation defines the data subject as an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number. As the definition of personal data was recently, according to the Decree 70/2011, amended in order to address under the applicable Data Protection Act, solely the data processing related to the individuals (excluding legal entities).

Principles

Principles related to the data processing are listed under the article 5 which mirrored the ones set forth in the Directive 95/46/EC with some branding new as (i) assertion of the transparency principle in data processing in relation to the data subject (this means that data subject would have to be told the purposes of processing and informed of their rights, what data is mandatory, the consequences of not providing data, the period for which data will be retained, if data will be exported and, if it is, how it will be protected); (ii) clarification of the data minimization principle (data processing is permitted if and as long as the purposes cannot

1 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on free movement of such data, European Commission, COM 2012 11/4 draft

be fulfilled without processing personal data); (iii) comprehensive liability of the controller (the controller shall ensure for each step of data processing its compliance with the Regulation).

Article 6 describes the lawfulness of the processing; in this respect the proposed Regulation reflects the spirit of the Directive. The so called "legitimate interests condition" allowing processing without data subject's consents, is preserved under article 6 (f) which allows the processing whenever is necessary for the purposes of the legitimate interests pursued by a data controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects who request protection. This rule together the article 7 slightly changes the basic approach of relying on consents given by data subjects. Specifically article 7 clearly states that the consent shall be "explicit" and if it is to be given in the context of a declaration which concerns another matter, the mandatory requirement is that the given consent "must be presented distinguishable in its appearance from this other matter".

The data subject shall withdrawn the consent at any time, irrespective if it is given by contract.

The article 7 closes with a statement according to which consent is not valid whenever there is a significant imbalance between the data controller and the data subject (this addresses a problem usually occurred in the relationship between employer and employee where the latter is used to grant a consent for a wider processing exceeding the basic purpose of the relationship).

Special categories of personal data are defined under Article 9 and in Articles 80 through 85; such special categories would include processing of personal data for, among the others, health purposes and historical, statistical scientific purposes. Specifically, according to the Article 83, personal data may be processed for statistical purposes only if:

(i) These purposes cannot be fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

(ii) Data enabling the attribution of information to an identified or identifiable data subject is kept separately from other information as long as these purposes can be fulfilled in this manner.

Rights of the data subject

Regulation has strengthened the transparency regime; specifically while the Directive required to provide information to data subjects about its personal data where necessary to ensure that the data processing is fair, the Regulation has extended such obligations, irrespective of any considerations concerning the fairness of data processing.

In this respect, both article 11 and article 14 specified that the controller is obliged to have transparent and easily accessible policies for processing data and for allowing data subjects to exercise its rights. In this respect, the controller shall provide any information in an intelligible, using clear and plain language adapted to the data subjects. Article 14 stated the minimum set of information that the controller must release are more or less the same stated in the Directive.

It is interested that the exception of the transparency are maintained also in the Regulation, which implies that the obligation of providing information to the data subjects will not be applicable if, among the others, the data are not collected from the data subject and the provision of such information proves impossible and would involve disproportionate effect. This specific exception is linked to the provision under comma 7 of the same article 14 according to which it is stated that the Commission shall be empowered to adopt delegated acts and the conditions and appropriate safeguards for the exception mentioned below.

This authority is conferred to the Commission also for further specifying the criteria for the further information necessary to guarantee fair processing in respect of the data subject.

It must be noted that comma 7 opens to some uncertainty as the Commission is called to adopt further acts; furthermore this should be linked to the comma 5 (d) according to which the exception of the transparency applied whenever the data are not collected from the data subject and the provision of such information will impair the rights and the freedoms of others, as defined in Union law or Member State law. Therefore, such exception may create improper and disqualified effects for the data subjects as the Members may define some particular circumstances, according to the law, in which data subjects need not be informed of personal data collected. This approach has two negative effects: the first one is to assign to Member States the right to specific sector or events for which the data subjects do not have full rights; the second effect is that data subject will have impair rights in comparison to other data subjects living in other Member States.

Article 17 introduced a particular right of the data subject so called "right to be forgotten"; this kind of right exists especially where processing is justified based on consent or contract, or where an individual wishes to remove data posted as a child. In this respect, the data subject has the right to obtain from the data controller the erasure of his/her personal data when – basically – the data are no longer necessary in relation for the purposes for which were collected and/or in the event of withdraw of consents by the data subjects. According to this disposition, if the controller made such data public it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, informing third parties which are processing such data, that a data subject requests to erase links or copy or any other replication of personal data.

Comma 4 of the article 17 defines the conditions according to which, instead of erasure, the data controller could apply restrictions in processing personal data where, for example, data are contested by the data subjects or when the processing is unlawful or when the controller no longer needs the personal data but such data must be kept as a proof.

Also in this respect the Commission is called to publish delegated acts for further specifying the conditions for deleting links as well as the conditions and criteria for restricting the processing of personal data.

Despite the fact that this article analyses the last draft of Regulation available, if the legislator wants to keep the need to await developments over legislative process for regulating, then, this could affect the overall implementation of this new legal framework.

Article 18 affirms a data portability right which assigns to the data subject the right, where the personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of such data. This right supersedes any confidential obligations or intellectual property rights of the controller. Despite the fact that such data could be in a format which could integrate an intellectual property right or could include also some information covered by confidentiality, the data subject has the right to request such data and to transmit them to another controller or automated processing system.

The other rights are addressed under article 19 and article 20: specifically the data subject has the right to object to the use of automated-decision taking techniques unless the controller shows legitimate grounds which override the interests or fundamental rights of the data subject. **The data subject shall have the right to object free of charge to the processing of personal data for marketing purposes and this right shall be offered to the data subject in an intelligible manner and it shall clearly distinguishable from other information.**

Any natural person shall have the right to be not subject to a measure which produces legal effects or is based solely on automated processing intended to evaluate certain personal aspects regarding his/her person or to analyze or predict

the natural person's performance at work, health, economic situation, reliability or behavior.

Controller and processor

Controllers and processors are to be required to document the data processing tasks in more detail; specifically the Regulation imposes to have a documentation in which detailing, among the other things, the purpose of processing, the description of categories of data processed, the description of recipients of personal data, the modality of data transfer abroad. Such documentation is not needed whenever the controller is a natural personal who processes data without a commercial interest and in the event of an enterprise who is employing fewer than 250 persons whenever the data processing is an ancillary activity. The Commission may reserve the right to lay down standard forms for such documentation.

Controllers would be required to take measures to comply with the new rules and must be able to demonstrate this. Every processing operation would need to be documented and the documentation must be available to authorities on request. Processors will need the consent of the controller to appoint sub-processors (while until now current legislation assigned this right solely to the Controller; processors could appoint solely persons in charge). The Regulation, also, specifies that if a processor process personal data other than as instructed by the controller, then the processor shall be considered controller in respect of that processing.

The Regulation will continue to apply to processing carried out by or on behalf of EU operations. However, the Regulation specifies that for those controllers with no EU establishment where they undertake processing related to offering of goods/services to EU residents, or which monitors data subjects resident in the EU, then, such controller are required to appoint a local representative, against whom enforcement action may be taken. This rule has several exceptions: as for example, it is not necessary whenever the controller established in a third country where the Commission has decided that such country ensures an adequate level of protection or a controller which offers occasionally goods and services to data subjects in EU.

The draft Regulation does not provide any provision regarding the current filing system. Therefore, it is supposed it will not exist anymore. However, 'risky' processing shall be subject to prior authorization by data protection authorities. Risky processing could include processing using new technologies (monitoring publicly accessible area using optic-electronic devices), or processing that could deprive data subjects of the benefit of a contract (a systematic and extensive evaluation of personal aspects relating to a natural person or for analyzing or predicting in particular natural person's economic situation, health, personal preferences, behaviors or reliability). Then the controller in these cases, is obliged to make an assessment which includes a general description of processing operations, of the risks and measures to be taken for reducing risks' impacts. In some cases, the controller or the processor (then the processor assumes a large scale of obligations in this respect) shall obtain a prior authorization from the supervisory authority, prior to a particular data processing, for ensuring the compliance of the intended processing with the Regulation and for mitigating the risks involved by the data subjects. This prior authorization is advisable especially for the "risky processing" as illustrated above and the supervisory authority could block such processing, imposing appropriate proposals for remedy, whenever it noted any incompliance with the Regulation. It

is also stated that the supervisory authority shall list processing operations which should be subject to such prior consultation/authorization and such list shall be provided to the European Data Protection Board.

Whenever such risky data processing affects several members' states then supervisory authority shall apply the consistency mechanisms set forth in article 57 and the members state shall consult with the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament in order to ensure the compliance of such processing.

Transfer of personal data to third countries or international organizations

It must be noted that the Regulation does not change the approach of the existing Directive, opening to a permissive regime which may impose prohibition in data transfer on case-by-case basis where particular risks are identified.

However, Regulation assigns a special role to the binding corporate rules, as per the article 43, expanding the concept so that binding corporate rules can be put in place by processors as well as controllers and requiring data protection authorities to approve them on the condition that such rules meet fairly limited criteria. The criteria will be determined by the Commission and authorities shall be obliged to inform each other authorities and the Commission and both of them have the right to object before approving such rules. This helps in order to address some legal problems in some members' states however this does not solve the problem of the approval under the relevant and competent authorities.

According to article 42 it is possible that a controller or a processor may transfer personal data to a third country or an international organization only if the controller or processor has adduced appropriate safeguards which could be, among the others, standard data protection clauses adopted by Commission or adopted by a supervisory authority in accordance with the consistency mechanism of article 57.

The Regulation also introduces, according to article 44 (1) (h), the transfer of data towards a country which does not have appropriate safeguards, whenever it is necessary for legitimate interests pursued by the controller or by processor which cannot be qualified as frequent or massive and where the controller or the processor has assessed all the circumstances surrounding the data transfer operation and based on this assessment adduced appropriate safeguards with respect to the protection of personal data.

It is clear that only the **Commission, as per the article 41, could evaluate that a particular jurisdiction ensures an adequate level of protection for personal data**. In this respect, UK controllers who frequently transfer data to a non – EEA processor without the need of a contract in the appropriate Commission form, relying on the fact that jurisdiction at which controllers are located can reasonably be taken to ensure an adequate level of protection, will be prevented in keeping this approach.

Consistency

This mechanism has been implemented in order to monitoring the application of the Regulation and for contributing to its application throughout the European Union. It is stated that before each supervisory authority adopts a measure, it shall communicate the draft measure to the European Data Protection Board and the Commission for their opinion.

Solely in the event there is an urgent need to act in order to protect the interests of data subjects, then the supervisory authority may derogate to the consistency mechanisms and adopt immediately provisional measures with a specific period of validity. At the same moment,

the supervisory authority may also request an urgent opinion to the European Data Protection Board. It is also clarified that an enforceable measure adopted by a Member State shall be enforce in all Member States concerned. This implies a serious issue as we could be in the situation that what is acceptable to a Member State could be unacceptable processing for other member states.

Sanctions

Sanctions mechanisms and their function are reported in several different section of the Regulation which introduces the statutory audit right by data protection authorities in order to investigate and assess if the controller and the processor comply with data protection rules (article 53). In addition specific fines may be imposed by each data protection authorities under the Regulation to the extent that (i) there is an intentional or negligent failure to comply with some specific data subject rights and the fine will be up to 0,5% of annual worldwide turnover; (ii) there is an intentional or negligent failure to comply with some specific data subject rights (as but not limited to not providing of information or provision of incomplete information, not providing access for the data subject or not complying with the right to be forgotten or to erasure of the data subject) and the fine will be up to 1% of annual worldwide turnover; (iii) there is an intentional or negligent failure to comply with the key requirements of the Regulation (as but not limited to processing data without any legal basis for processing or processing special categories of data infringing the requirements) and the fine will be up to 2% of annual worldwide turnover;

In case of a first and non intentional non compliance with the Regulation a warning in writing may be given and no sanctions shall be imposed where (i) a natural person is processing data without a commercial interest; (ii) an enterprise employing fewer than 250 persons is processing data as an ancillary activity.

No clear rules have been provided on who will take the responsibility for enforcing the Regulation against controllers and processors established outside EEA. In addition whenever the Regulation refers to the annual turnover it is referring to the turnover of the concerned company and not to the one of the consolidated group of entities to whom the company may belong.

It seems that the sanctions mechanism and auditing procedure implement a complex system which lead attention and resources to be addressed by controllers and processors for being in compliance with the data protection rules.

The Proposed Regulation will now enter an evaluation and discussion phase by the European Parliament and Member States. The Regulation is viewed as a positive effort to standardize rules for all European Union members but at the same time, it takes also problems in terms of independency of European Data Protection Board versus the Data Protection Authority and also in terms of implementing measures by the companies in order to avoid potential liability. Measures aimed to monitor, to enhance internal procedure, to mitigate any risk of data breach