GDPR: Not an easy birth for the Record of Processing Activities

by Gloria Marcoccio/gloria.marcoccio@glory.it,

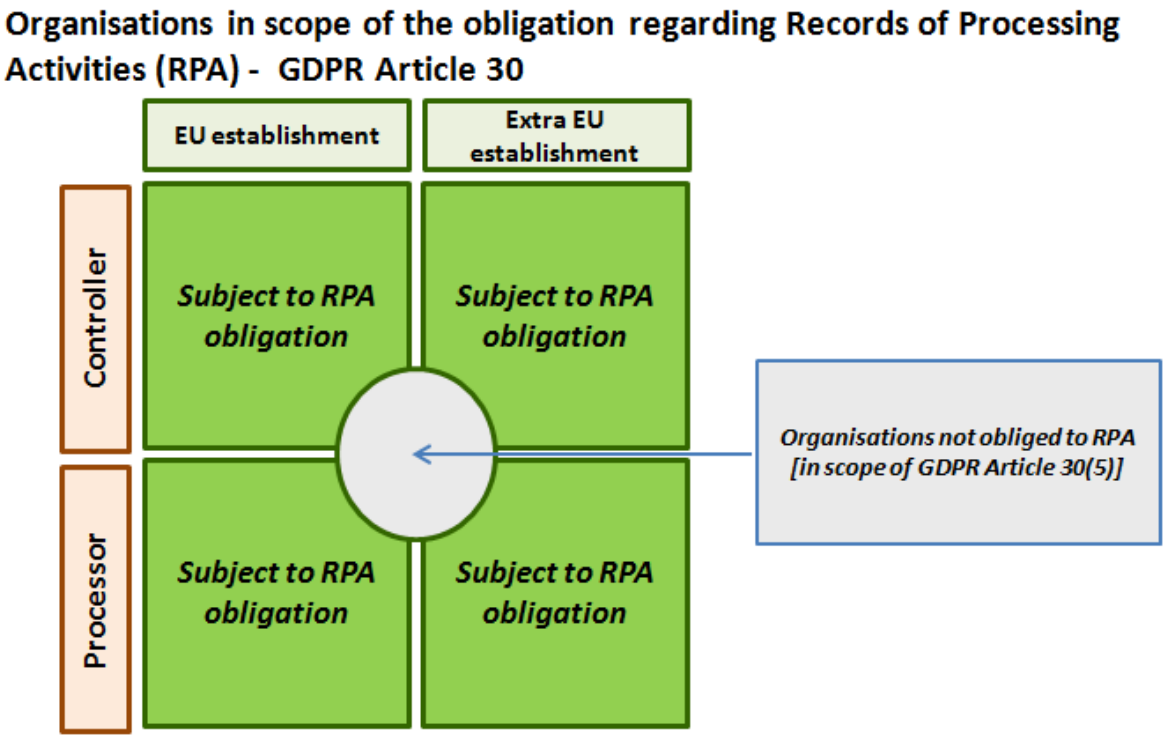
July 15 2017

The time for starting the preparation of the Records of Processing Activities in compliance with GDPR Article 30 is coming for many Organisations: all is it clear about it? Maybe not.

With regards to the new provisions brought by the GDPR the attention has been obviously focused, among the other, on Data Breach (GDPR Articles 33, 34), Data Protection Officer role (GDPR Articles 37-39) and Data Protection Impact Assessment (GDPR Articles 35,36) since they have heavy impacts in terms of required technical and organisational measures and first of all, related budgets. Comparing with such provisions, the requirements about Records of Processing Activities (RPA) could appear as ancillary measures, however this is not true. In fact RPA is fully part of what is necessary to set up and keep updated in order to be compliant with the Accountability principle (GDPR Article 5(2)) and it also represents the connecting ring between the Organisation data protection management system and the external world made by:

- Supervisory Authority requests of accessing the RPA
- congruence with the information reported in the Privacy Notices towards the Data Subjects

RPA in gross terms is going to replace the 95/46/EC obligations about the Notification of personal data processing from Controllers to the relevant national Supervisory Authority. The level of granularity of the RPA information required to set up and managed seems not be very detailed, however a number of possible pitfalls emerge when an Organisation starts its work about RPA.



How many Organisations out of RPA scope?

Not so large the number of Organisations not obliged to set up and manage their RPA: the RPA provisions do not apply if fewer than 250 persons are employed unless the processing carried out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in GDPR Article 9(1) or personal data relating to criminal convictions and offences referred to in GDPR Article 10.

This means that the Organisations employing fewer that 250 employees (and the head-count should consider all the type of contracts between employer-employees...) have to perform in any case a risk analysis aimed at identifying whether their processing involve risk to rights and freedoms of individuals and to manage a map of the personal data processed so as to be able to detect whether they process special categories of data or data related to criminal convictions and offences, and must be able to document such information in compliant with the Accountability principle (GDPR Article 5(2)) . As a result, considering also the case of Small Medium Enterprises, it appears very limited the number of Organisations out of scope for the RPA.

EU and not EU Organisations

According to GDPR Article 3(2), the European Regulation shall apply also to Organisations (Controllers or Processors) *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; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.* This means that another wide set of Organisations, such the Social Networks or Payment Service Providers or On line behavioural tracking service providers (for marketing purposes or other) not established in the EU need to set up and keep updated their RPAs, regardless their role of Controller or Processor.

Controllers, Processors...and SubProcessors

The RPA provisions apply both to Controllers and Processors. In particular for the Organisations acting in the role of Processor RPA is another one of the GDPR provisions specifically addressed to them (together with: Security measures GDRP Article 32, Data Breach involvement GDPR Article 33,....) increasing their responsibilities& effort required as well as liabilities in front of the law (and relative exposure to sanctions, up to 10.000.000 eur or 2% worldwide turn over if higher).

Furthermore, according to the wording of paragraph 2 of Article 30, it seems sufficiently clear that the Organisations acting as Processor engaged by a Processor in processing personal data on behalf of a Controller, shall need to set up and keep properly updated their RPA, since they are still Processor of the Controller (according to GDPR Article 28(4)).

Then, it should be considered that many Organisations play both the privacy roles: Controller - at least with regard to their internal processing (HR management, company security, facilities management,...) and Processor insofar their business includes the provision of services involving processing personal data. As a result such Organisations shall manage two types of RPA: the type for their role of Controller (GDPR Article 30(1)) and the type for their role of Processor (GDPR Article 30(2)).

Last but really not least, the Organisations acting in the role of Processor, should by pay special attention in the preparation and management of the RPA since it shall contain information for each Controller: an hard work when the number of Customers-Controllers is high and when the panel of Customers-Controllers frequently changes.

The structure of the RPA and the need to standardize approach and information required

Athough not clearly stated in GDPR Article 30(1) the records in charge to the Controller should be organized considering also the categories of processing, as conversely clearly reported in GDPR Article 30(2), i.e. the records in charge to the Processors (...*shall maintain a record of all categories of processing activities carried out*...)

In any case it appears clear that recommendations should be given at EU level at the purpose of defining a common approach in order to report the information required by the RPA, at least for describing: *the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed*... *category of processing*....

Some European data protection Supervisor Authorities have already started to provide their national guidelines about the preparation of the RPA, as in the case of the French and the Belgian Data Protection Authorities, however this could unfortunately lead to jeopardisation and differences among EU countries, exactly the contrary of one of the main aims of the GDPR, i.e. to prevent fragmentation in the implementation of data protection across the Union.

RPA data retention issues

The provisions regarding the RPA seem to focus on the attention on the processing presently carried out by the Organisations but what about the 'old data' concerned by an RPA considering the need of the Supervisory Authority to access such information? In other terms how long previous releases of an RPA should be retained. It does no appear a responsibility of the Controllers and Processors to autonomously take a decision about the RPA retention since RPA comes out from a Supervisory Authority need.

In this sense a timely intervention by WP29 or the forthcoming European Data Protection Board would certainly be welcomed by the Organizations that have to meet the requirements about the RPA, in particular the international groups that could be obliged to set up and keep updated several country specific RPAs.