diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

An overview about sanctions provided for by the new European Regulation on personal data protection

Autore: Marcoccio Gloria
In: Diritto costituzionale

Introduction

The European Parliament, Council and Commission, after three years of intense and complex negotiations and revisions, in December 2015 reached an agreement on the final text of the new European General Data Protection Regulation (Regulation[1]): this is the most important change that will affect the laws regarding the protection of personal data in the EU,
20 years after the European privacy Directive 95/46/EC. The Regulation brings the acknowledgment of greater protection for the data subjects, general increased levels of personal data protection with the introduction of new security measures, new requirements, as well as substantial sanctions for infringement of its provisions. The Regulation shall be published in the EU Official Journal after its formal approval by the European Parliament in plenary session, event 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). The Regulation has significant impacts on businesses of all industries and will require careful review of the existing company privacy posture and rapid adaptation to the new technical, organizational and procedural measures.

There are many innovations introduced by the Regulation and those concerning the framework of sanctions are the subject of this short note and related considerations.

Common rules for administrative sanctions

First, we need to consider that the new European legislation, with its nature of Regulation, sets out a unique framework of sanctions
at EU level, designed to standardize as much as possible the approach for handling sanctions in case of infringement of the rules provided for personal data processing, so far an issue
inevitably and completely anchored to the provisions in this regard by the legal systems of
each single EU Member State. In fact, as a result of the provisions of article 24[2] Directive 95/46/EC, amounts of sanctions, provisions concerned, as well as procedures and criteria adopted by the European Data Protection Authorities (DPAs) for their application, show important differences and
particularizations at level of individual Member State. A few examples: in UK for serious violations of the Data Protection Act, the DPA may impose a fine up to 500.000 pounds (about 661.000 euro) whereas in Romania the level of sanctions is decided at the discretion of the Romanian DPA; the Italian situation in this regard is quite varied and taking as
reference the case of non-compliance with orders issued by the Authority, article162 (2-ter) of Legislative Decree 196/03, the Italian DPA may impose sanctions up to 180.000 euro, a value that can also be increased up to four times, where it is evaluated
ineffective because of the economic conditions of the offender (article 164-bis of Legislative Decree 196/03).

Key features of the sanctions provided for by the Regulation

Diritto & Diritti ISSN 1127-8579

In order to strengthen and harmonize at EU level the administrative sanctions in case of violation of the Regulation, the European DPAs are explicitly empowered to impose fines: for infringement of
specific requirements of the Regulation, with a certain maximum pecuniary value, according to a specified set of indications for determining the penalty to be applied in each individual case. This criterion considers a variety of factors including: the nature, severity and duration of the infringement, the number of data subjects involved and the level of damage they suffered, the categories of data subjects involved, the measures taken by the offender to prevent or mitigate the consequences of the infringement and the degree of its cooperation with the DPA, aggravating or mitigating aspects applicable to each specific case of violation.

Regarding the maximum amounts of fines, the European legislator has identified two separate categories taking into account
type of offender (person, undertaking) and type of infringed prescriptions. In summary, the resulting framework for administrative sanctions provided for by the Regulation can be schematically represented as follows:

Administrative fine up to 10 million euro, in case of undertaking up to 2% of the total worldwide annual turnover, whichever is higher) for infringement of provisions concerning:

child's consent in relation to information society services; security; accountability; principles of Privacy by Design and Privacy by Default; DPA Prior Consultation; obligations in general for the Controller, Processor and Representatives of Controllers not established in the Union; Data Breach; Privacy Impact Assessment; Data Protection Officer; privacy certifications (such certifications represent one of the essential news brought by the Regulation, see next paragraph)

Administrative fine up to 20 million euro, in case of undertaking up to 4% of the total worldwide annual turnover, whichever is higher) for infringement of provisions concerning:

requirements about
expression and documentation of consent; principles of fairness and lawfulness of the processing; the rights of the data subject (including the data portability and the right to be forgotten); data transfers extra UE; compliance with measures issued by relevant DPA; communication of Data Breach to the data subjects; compliance with specific prohibitions of treatment; compliance with the requirements for specific cases of treatment as those affecting the data of workers in the context of the work relationship

Well evident the strong tightening for the fines and the wide range of requirements involved of the Regulation. Therefore it will be essential that the application of such harsh sanctions regime will be made in an homogenous way and that does not become instead a source of new divergences between EU Member States: at this purpose the coordination between the European DPAs (expressly provided for by the Regulation) has crucial importance for the success and effectiveness of the new European regulations on personal data protection, hoping it can avoid imbalances that would be really difficult to justify from all points of view, and with obvious negative impacts on businesses as well as on the responsibility of the individuals.

Penalties

As regards the criminal aspects, the Regulation states it is the responsibility of each single EU Member State to determine the measures to be taken, in such a way that penalties to be applied must be effective, proportionate and dissuasive. With reference to the Italian case, it is envisaged, in principle, to hold the current framework of sanctions for criminal offenses outlined with the provisions in Articles 167 - 172 of Legislative Decree 196/03, with the necessary changes as a function of the new framework of obligations and requirements set out by the Regulation..

Applicability of sanctions for particular actors and the case of the public sector

Unlike Directive 95/46/EC, in addition to the Controllers the Regulation identifies other addressees of its requirements.

First of all the Processor (i.e. the entity that performs data processing on behalf of the Controller, it is typically a provider of services involving personal data processing): such privacy role is already defined by Directive 95/46/EC, however whose responsibilities
are now greatly broadened since it is explicitly addressee of obligations in terms of: need to define a representative in the EU for the purpose of the legislation in question (if the Processor is established in country extra EU), obligations to inform the Controller
and achieve its consent should the Processor intends to involve subcontractors in personal data processing operations (they will be additional Processors), obligations to constrain such additional Processors to comply with the instructions provided by the Controller, maintaining appropriate documentation about treatments carried out (the concept of accountability), obligations to cooperate with the DPA
when required, obligations to implement security measures, reporting without undue delay to the Controller in case of Data Breach, obligations to appoint the Data Protection Officer in certain conditions (the same applicable to the Controller), compliance with the certification rules if the Processor adopts a certification for purposes of processing personal data, obligations in
case of transfer of data to countries extra UE.

These increased responsibilities
evidently entail greater exposure to risk of sanctions also for Processors in addition to the Controllers..

Then there is the case of the Certification body. The Regulation introduces an important innovation: the (voluntary) certification and adoption of 'privacy seals' in order to demonstrate compliance with the Regulation in the data processing activities carried out by Controllers and Processors. The introduction of certification for the purposes of privacy legislation is undoubtedly destined to arouse great interest:

- in positive, since it opens a market very innovative and wide; furthermore introduces benefit for

companies because the adoption of such 'privacy certifications' will involve, at least, less red tape (bureocracy is reduced, but still inevitably present in the Regulation)

- as an element of concern from various points of view, considering the bond that is created between performance required as a legal obligation and a statement to this effect based on a certificate issued by a third party. This approach could present some 'logic' flaw and also result in negative consequences likely to compromise the entire system of setting privacy certification

Then the Regulation identifies specific tasks and requirements for institutions involved in the certification mechanism and related maintenance (certification bodies and relevant control bodies), in violation of which it is provided against such entities a sanction up to 10 million euro (or up 2% of turnover in case of an undertaking, if it is over 10 million eur).

With regard to public authorities and bodies, the Regulation leaves to the EU Member States the determination about whether and to what extent the administrative sanctions can be imposed to such authorities and bodies: on this point the approach is quite different from the one followed with Directive 95/46/EC well depicted by its recital 55 ".... whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive" and its Article 24 did not introduced any specific treatment for the case of sanctions for violations committed by the public administration (see footer note 2).

Diritto & Diritti ISSN 1127-8579

The wide territorial scope of
the Regulation and consequent number of addressees of sanctions for failing to comply with its provisions

One of the key features of the Regulation, which has been target of several criticism and change requests from major international operators of services based on personal data processing (social networks, sale of goods and services via the Internet, non-EU suppliers of various services such as 'data hosting', advertising companies ...) is certainly
the wide scope of its application: in fact, besides being applicable to companies (Controller, Processors) established in the EU with their business activities, the Regulation also apply to companies (Controllers, Processors) not established in the EU, who:

- process personal data of individuals who are in the EU (not necessarily only resident in EU countries) and the processing is in connection with offers of goods or services, regardless of whether or not a payment is required for them,

and / or

- perform monitoring on the behavior of these people (online behavior in the Internet but also other monitoring, for example in the use of goods and services) to the extent that the behavior under monitoring takes place within the EU

While bearing in mind the existence of margins for the literal interpretation of the provision regarding the scope of applicability of Regulation (for example, how to delimit and detect, in a way documented and

enforceable against third parties, a 'behavior within the EU ' when activity is carried out via the Internet by the person), in any case
the number of addressees of the provisions about sanctions provided for by the Regulation will be much wider
than the one existing with the current legislation: we shall see. after the next two years and in practice, how the authorities will actually be in a position to detect violations and impose sanctions for recipients belonging to such
territorial scope more than wide, boundless.

[1] This note 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/

[2] Directive 95/46/CE - Article 24 Sanctions "The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive."

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

Diritto & Diritti ISSN 1127-8579