"One -day training on GDPR"

November 15th, 2019 – Larnaca, Cyprus

The experience of the Italian Court of Auditors in implementing G.D.P.R.

– draft –

1. This essay is aimed to provide a general idea of the experience of the Italian Court of Auditors in implementing G.D.P.R. Basically, this implementation can be examined under two different perspectives: 1) an **internal** one, connected to the storage and management of data by the Court; 2) an **external** one, involving third parties to whom personal data are referred. This second perspective opens two different field of examination: i) what happens, after G.D.P.R. has entered into force, to data collected before; ii) which are the implication of G.D.P.R. to future activities of data collection performed by the Court.

2. In examining the defined questions, it has to be considered that Italy has adopted a specific legislative act – the legislative decree no. 101/2018, entered into force on September 19th, 2018, in order to harmonize the old "Italian Privacy Code" (legislative decree no. 196/2003) and other national laws dealing with this subject matter with the European General Data Protection Regulation. Even if an E.U. regulation, being "self-executing", does not need any formal implementation by national laws, this choice of the Italian legislator has depended upon the necessity to imprint an higher coherency to the system of protection of personal data, as also

progressively defined by the competent national Authority in its decisions. Therefore, it has been used the "regulatory empty space" left by U.E. to Member States on this subject matter to provide for complementary regulation regarding particular categories of personal data, among which the judicial ones. The regulatory set, consequently, is spread between G.D.P.R. and these others provisions of law, which, on the other hand, are today consistent with the G.D.P.R. itself.

3. With regard to the above-mentioned "internal perspective", the Court of Auditors has adopted the so-called "cloud first" principle and, abandoning the idea to manage a physical data-center, has implemented a system of public cloud as a preferential technological tool for the related services, also connected to data management. This implementation of the public cloud, declined on models of delivery "SaaS" (Software as a Service) and "(PaaS)" (Platform as a Service), has led the Court of Auditors to define its own security framework both under rigid international standards, such as ISO/IEC 27001:2013 and Enisa's "Cloud Computing Information Assurance Framework", and under Italian/European standards, according also to the mandatory requirements of the G.D.P.R. In this perspective, the Court of Auditors has developed its own Cybersecurity system and is constantly able to determine precisely where specific data are hosted and on which components of the chain of applications they are transiting. All the suppliers involved are therefore designated as external data processing managers and bounded, by provisions of contract, to grant a full respect of G.D.P.R., in all the aspects concerning the access, transfer, storage and secure deletion of data present in the infrastructure of the provider of cloud service.

4. With regard to the above-mentioned "external perspective", involving third parties whose personal data are referred to, it has to be remembered that The Italian Court of Auditors, supreme auditing institution of the Republic, is part of the

jurisdictional branch under articles 100, 2nd par., and 111, last par., of the Constitution; besides specific jurisdictional functions, it also exerts, in its different Chambers (central or regional ones), control on the legitimacy of acts, on budget of public administrations, on management and performance of public entities – i.e., according to ISSAI 300, paragraph 9, an "independent, objective and reliable examination of whether government undertakings, systems, operations, programs, activities or organizations are operating in accordance with the principles of economy, efficiency and effectiveness" – and control on the utility of public policies (see, among recent ones, judgments no. 1/SSRRCO/AUD/19; 15/SSRRCO/AUD/18; 13/SSRRCO/AUD/18). In the Court of Auditors a General Prosecutor's Office is also instituted, mainly in order to prosecute civil servants for damages to public administration.

4.1. Under article n. 23 of G.D.P.R., it is possible to restrict "the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5" in so far as "such a restriction" – which has however to respect the essence of the fundamental rights and freedoms – is "a necessary and proportionate measure in a democratic society to safeguard (…) (f) the protection of judicial independence and judicial proceedings", especially the ones related to the investigations of Prosecutor's Office. Therefore, it is necessary to move first of all to these specific regulations concerning judicial activities, under art. 23 of G.D.P.R.

According to article n. 52, first and second par., of legislative decree n. 196/2003, in a judicial procedure the interested party is always permitted to ask, for legitimate reasons, by a request filed at the Chancery of the proceeding Court, the deletion of the indication of identifying data from all the copies of the judgment, but the original one, in case of reproduction. The same deletion can be ordered, *ex officio*, by the proceeding judicial authority (sometimes this is a specific duty, *see* article n.

734-*bis* of the Italian criminal code, for cases of sexual crimes involving minors). Therefore, further dissemination of the judgment has necessarily relevant personal data omitted.

If, accordingly, jurisdictional functions of the Court of Auditors enjoy a special status with regard to the duties set by G.D.P.R., also chambers invested of functions of control are in a peculiar position, even when these activities are not performed with jurisdictional procedures; this for substantial reasons. The Court of Auditors, in these procedures, substantially controls administrative branches and refers the results of the controls to the elected assemblies invested of the constitutional mandate of controlling the same branches; therefore, in its activities of control, the Court supports constitutionally relevant functions of Parliament, regional and municipal councils; in fact, public administrations involved in the procedures of control are requested to adopt, according to the law (no. 20 of 1994, art. 3, 6th par., as amended), within six months from the date of notification of the final decision, all the necessary consequential measures, which have to be communicated to the Court and to the *interested legislative branches*. It is hard to imagine, in such a context, a refusal of transmission of data based on G.D.P.R., especially considering that activities of control potentially interfering with third parties' rights usually require extreme aggregated data, often in a statistically relevant dimension: therefore the refusal could not be motivated on the basis of a public administration's direct interest, because of the constitutional position of the administration itself; it could not be motivated on the basis of a private party's direct right, because of the level of aggregation of data with which control usually deals.

4.2. If these rules applies since few years ago, the General Secretariat of the Court has searched to deal with the same problems with regard to the past. By order

n. 5209 of May 24th, 2018, the Secretariat has in fact ordered the anonymization of *all the judgments* displayed in the database on the internet under some circumstances.

In particular, there were some judgments on pensions of civil servants containing data suitable to reveal the health state of the interested parties, not correctly deleted. The Secretariat has ordered the anonymization of the published judgments, independently by the judicial order under article n. 52 of legislative decree n. 196/2003, in all the cases in which: (a) personal data permitted to identify minors or specific familiar status or relationships; (b) data were suitable to reveal the health state of a person; this on the basis of previous Italian Privacy code, enforcing U.E. directives.