

**Overview of the Implementation of the Italian Personal Data Protection Code**

**Annuale Report 2019 - Executive Summary**

* 1. *Between continuity and innovation:* this slogan could sum up the activities of the Italian supervisory authority in the past year. As we all know, the General Data Protection Regulation (GDPR) has been in application since 25 May 2018; the year 2019 proved to be, for all stakeholders, a time of testing and stepwise adjustments. This also applies to the Garante: indeed, whilst the members of its collegiate panel remained in office on account of subsequent regulatory measures, which were of late also grounded in the supervening health emergency (see paragraph 2.2, No 1), the Authority as a whole worked on several levels. In the first place, the activities focused on the general public and the multifarious stakeholders impacted by personal data protection legislation, who were reassured as to the (mainly) seamless transition from the previous legal framework – based on transposition of Directive 95/46 – to the new one created by the GDPR; clarifications were provided via the most diverse channels on the innovations brought about by the EU instrument.

Following up on the requests made by individual entities and trade associations, the Garante highlighted the continued validity of a considerable portion of the decisions and measures adopted in the past years. This is the case, for instance, of benchmark indications provided by the Garante in several areas – often by way of guidelines and general application measures that have been put to test successfully in many respects – including banks (paragraph 1.4.2), use of the Internet and email at the workplace (paragraph 14.4), and even the management of condominiums (paragraph 15). It can easily be grasped that these are issues impacting substantially the implementation of personal data protection legislation in daily life as well as the standard operation of businesses and public administrative bodies. From this perspective, the criteria for distinguishing the right to access personal data from other types of access envisaged in our legal system were reaffirmed - for instance, regarding banks and insurance companies; as for the latter, the focus was placed especially on access to the personal data contained in forensic medicine reports and the relevant limitations, with particular regard to subjective evaluations and judgments as contained in those reports (paragraph 14.2). The Authority also recalled the principles applying to the processing of personal data in connection with due diligence procedures as required by the applicable anti-money laundering laws, or in the course of advisory services provided by banks and investment companies in order to assess adequacy and appropriateness of operations or services to customers (paragraph 14.2).

Clarifications were also provided regarding the innovations brought about by the amendments made to the Code (paragraph 13.7) in terms of limitations on the exercise of data subjects’ rights, processing of data concerning health (paragraph 5.2), or the employment sector – such as the duties and responsibilities falling to professionals that process personal data on the employer’s behalf (paragraph 13.6) or the processing activities carried out by appointed doctors (paragraph 13.14).

* 1. These dissemination activities, which have featured from the start among the key tasks of data protection authorities, have been implemented without sparing resources and energies and by relying on all methods and channels for official communication. Thus, the Authority’s front office continued to provide upfront information and replies (see paragraph 23.5 and the helpful breakdown of the workload in Table 12 of Part IV), whilst communication activities were implemented like in the past via the information and multi-media products developed by the Office and through the continuously updated website (Chapter 23 and Table 2 of Part IV). The GDPR provided an opportunity to shed special light on the interactions with data protection officers as part of two EU-funded projects (‘T4DATA’ and ‘SMEDATA’) (paragraph 21.15), DPOs being key pillars to foster the effectiveness of data protection legislation both in the view of the EU legislator and from the perspective of supervisory authorities (see paragraphs 4.9 and 5.4.3). In-depth analyses and leading-edge issues were addressed as well including via the contributions given by the members of the collegiate panel participating in several conferences and events (paragraphs 21.4 and 23.5).
  2. However, it is in the collaboration with other institutions where the ‘advisory’ role played by the Garante took on special importance, following the obligation to consult with the Authority (introduced by Article 36(4) of the GDPR) as part of the process leading to the enactment of primary legislation - if such legislation is liable to impact personal data protection rights – on top of the consultation relating, like in the past, to all types of secondary legislation. In discharging this task, the Garante set up or continued fruitful institutional relations in many areas and respects. Further details can be found in the text of the Annual Report, including the list of the opinions rendered (see paragraph 3.1 and Tables 3-5 in Part IV). Here reference can be made to the frequent interactions with the Ministry of Health regarding the operating arrangements of highly sensitive information systems such as the Transplantation Registry, the National Registry of reproductive cells donors for medically assisted heterologous reproduction, and the Infectious diseases alerting system; the implementation of the electronic health record (paragraph 5.2); or the issues concerning the so-called ‘living will’ (paragraph 5.3). By the same token, implementation of the so-called pre-compiled ISEE (Equivalent Economic Situation Indication) declaration as required from candidate beneficiaries of economic aid and the complex processing operations underlying functioning of the national basic income scheme required continued cooperation with the Ministry of Labour and Welfare (paragraph 4.2). Frequent as well as fruitful interactions were held with the Revenue Agency with regard to the complex processing operations in the relevant sectors – see, in particular, those related to the so-called ‘receipt lottery’ (paragraph 4.5). This accounts for the substantial number of opinions issued in the past year concerning the most diverse areas as well as for the frequent contacts between the Garante and Parliament (paragraph 3.1.4).

Unquestionably, one has reason to be satisfied in view of the account taken of the Authority’s positions and suggestions, which were taken up to a considerable extent also during the preparatory activities carried out most usefully in the various working groups; still, the guidance provided by the Garante was sometimes overlooked even when focused on key components of data protection legislation – including the need to respect the proportionality principle and the statutory obligation to minimize personal data in processing activities as well as in configuring increasingly complex and networked IT systems. These principles were actually left out in certain cases. Reference can be made to the extended retention period (until at least the 31st of December of the eighth year following submission of the relevant income report) set out for the personal data contained in electronic bills, which also include information on nature, type and amount of the goods and services purchased; additionally, it will be possible to use the billing data for the purposes of all the financial controls carried out by the Financial Police (paragraph 4.5.7). The same applies to the concerns raised by the Garante in respect of the processing of biometrics associated with video surveillance to monitor employee attendance in the public sector (paragraph 13.12).

* 1. No less demanding was the ‘advisory’ role played by the Garante in connection with the numerous opinions (see paragraph 4.3) issued on FOIA-type access requests following the inquiries made by transparency and anti-corruption officials and ombudspersons. This issue actually reflects the overarching tension between the legitimate requirements of administrative transparency and the need to respect personal data protection rights. In the past year, one of the main areas where such tension surfaced was the judgment No 20 of 23 January 2019, whereby the Italian Constitutional Court found that Section 14(1-a) of legislative decree No 33 of 14 March 2013 (regulating FOIA-type access) was in breach of constitutional principles (see also the 2018 Annual Report, paragraph 1; see paragraph 20.3 below). In that respect, reference should be made to the somewhat halting ‘response’ provided by Parliament via decree-law No 162 of 30 December 2019, which is expected to be implemented in full through an ad-hoc governmental regulation.
  2. As already pointed out, the GDPR did not result into sudden U-turns or leaps in the dark; however, the provisions adapting the national legal system to the GDPR as set forth in legislative decree No 101/2018 did commit a number of major tasks to the Garante in order to enable a ‘seamless’ transition from the old to the new regime. One such task was bringing about the ‘transformation’ of the pre-existing codes of ethics and professional practice concerning business information systems and credit reporting agencies into codes of conduct in line with Articles 40 and 41 of the GDPR; that transformation was to be finalised within the 19th of September 2019 as per Section 20 of legislative decree No 101/2018 (paragraph 14.3). Yet another example in this regard is provided by the need to determine which provisions out of those contained in the pre-existing general authorisations to process ‘sensitive’ data were compatible with the new legal framework; this was done by way of a general application decision which was the subject of a public consultation (decision No 146 of 5 June 2019, web doc. No 9124510 – see paragraphs 5.5.1 and 13.2).
  3. Inspection activities continued partly thanks to the valuable contribution provided by the Special Privacy Protection and Technological Fraud Unit at the Financial Police, albeit by taking account of the new legal framework and the requirements to be met by all the stakeholders in order to adjust to the GDPR (paragraph 18.2). Those activities were focused in part on areas that have become staple components of the Authority’s workload over the years. As regards, in particular, certain business practices that fall short of personal data protection rights (such as the activation of unsolicited contracts) and telemarketing, special attention should be paid to a few decisions by the Garante that stand out because of the hefty fines imposed – the highest ever since establishment of the Authority (paragraphs 10.1, 11.1 and 14.5.2). Reference should also be made to the fine imposed jointly on Facebook Ireland and Facebook Italy on account of the infringements found within the framework of the investigations into the notorious ‘Cambridge Analytica’ case, which involved Italian nationals and brought to light the possibly serious impact of the online processing of personal data not only on the individual sphere, but also on the unfettered expression of people’s will in the course of electoral processes (see paragraphs 11.3 and 19.2).

However, in-depth investigations (see, for an overview of the sectors where alerts, complaints and queries were received in 2019, Tables 10 and 11 in Part IV) and inspections by the Garante led to the adoption of several decisions in many additional areas (see paragraph 18.4) so that sanctions were imposed, for instance, on account of the unauthorised use of data concerning health for purposes other than the treatment-related ones that had legitimated data collection (paragraph 5.1.1); the unlawful communication of such data due, among others, to mistakes made in forwarding the relevant documents (paragraph 5.1); and the violation of data subjects’ rights in the course of journalistic activities (paragraph 8.3) – which issues were addressed in a meeting with the Chair of the National Board of Professional Journalists (paragraph 8.2). Controls were also carried out on the appropriate configuration of increasingly used apps and the use of the data generated by those apps (see paragraphs 5.1, 11.1, 4.6 and 13.8); the use of apps was actually the focus of the 2019 Privacy Sweep (paragraphs 21.3 and 23.1).

* 1. One cannot fail to mention, as part of the transition experienced in the past year, the work done by the Garante in organisational terms, in particular by revising and restructuring the internal rules of procedure No 1/2019 and 2/2019 (see web docs. No 9107633 and 9107640, respectively). This work allowed adjusting the Garante’s *modus operandi* to the new legal framework and was translated operationally into developing the information systems relied on; this in turn made it possible to implement the Authority’s ‘digital switch’ thanks to the key commitment shown by its technological unit and enabled the Garante to continue working seamlessly and securely also during the lockdown period (paragraph 25.5).
  2. The adjustment to the new legal framework was actually not limited to the national arena. On the one hand, the Garante participated in the cooperation activities with other European SAs related to supervision over cross-border processing activities – first and foremost through the IMI (Internal Market Information System) platform, which has by now completed its run-in phase. Those cooperation activities increased considerably the workload of various departments in the Authority (paragraphs 11.4, 14.6, 16). On the other hand, the Garante contributed unceasingly, in many different ways, to the work of the European data protection Board including through participation in various expert groups (paragraph 21.1 and Table 16).

The Board continued working on guidance and documents intended to clarify key notions of both the old and the new European legal framework concerning data protection. This led to adoption of the guidelines on the processing of data required for performance of a contract concluded with the data subject (Article 6(1), letter b), which legal basis is especially relevant in connection with the provision of online services), the guidelines on the territorial scope of application of the GDPR, and the updated WP29 opinion on the notions of data controller and data processor. The innovations introduced by the GDPR were also addressed, in particular via the opinions on the processing activities for which a data protection impact assessment is required, the guidelines on codes of conduct and certifications and on data protection by design and be default; new guidance was provided on long-debated issues such as video surveillance – which was addressed by a new opinion taking account of the latest available technology – and the exercise of the right to be forgotten vis-à-vis search engines (paragraph 21.1), the latter being an area tackled by the Garante on several occasions as well (paragraph 8.5).

Like the Garante, the Board worked on adjusting its own Rules of Procedure, which were revised three times during 2019; additionally, a new Coordinated Supervision Committee was set up within the Board to enhance cooperation among supervisory authorities in the oversight over the bodies, agencies and offices operating in the areas related to borders, asylum and migration (SIS, EES, ETIAS, VIS), judicial and police cooperation (SIS, EPPO, Eurojust, ECRIS-TCN) and the internal market (IMI) (paragraph 21.2).

Nor did the Board fail to contribute to the review of the GDPR the European Commission is tasked with performing firstly within 25 May 2020, pursuant to Article 97 of the GDPR, and every four years thereafter. This first review concerned, in particular, the implementation and functioning of Chapter V on international data transfers to third countries or international organisations and Chapter VII on cooperation and consistency procedures. Having taken stock, albeit summarily, of the cooperation activities by national supervisory authorities, the Board issued a favourable judgment regarding this initial implementing period of the GDPR and considered it premature to put forward amendment proposals; conversely, the timely adoption of the new e-privacy regulation was found to be necessary in order to complete the EU data protection legal framework.

Innovation was key also for the Council of Europe and OECD: the former achieved the signature by sixteen new countries, including Italy, of the Protocol amending the 108/81 Convention, which gave rise to the so-called ‘Convention 108+’; the latter started revising the OECD Privacy Guidelines, whose current version was adopted in 2013 (paragraph 21.3).

* 1. In the coming years, cooperation is bound to be one the pillars to achieve effective protection of fundamental rights and digital security – as shown by the data breach notifications submitted to the Authority, see paragraph 16. This will include fair cooperation first and foremost with data controllers, leveraging on the many accountability and interaction tools that are envisaged in the new legal framework – codes of conduct, consultation of the supervisory authority following an impact assessment, certifications, DPOs. It will also entail reinforced cooperation with national and international technical standards organisations (paragraph 22) and, obviously, other supervisory bodies – including those outside the data protection area. Indeed, as shown by the joint investigation that was carried out with the Italian Authority for Communications Safeguards and the Italian Antitrust Authority regarding big data, which yielded a piebald picture as better detailed in the final report of that investigation (web doc. No 9264297), other national sector-specific authorities will have to be involved as they are also impacted by the challenges raised by technological and economic developments. This is aimed ultimately at overcoming any limitations possibly resulting from a silos mentality as applied to the discharge of the respective tasks – which would be beneficial in the first place to the stakeholders’ community.
  2. The big data dimension, more generally the issues related to the data economy and the increasingly blatant risks caused by the commodification of personal data (see paragraph 11.2) - compounded by the so-called ‘surveillance capitalism’ - point to the future fields of work for data protection authorities, mainly in connection with the rise of artificial intelligence and the algorithmic assessment of our lives. This is where urgent action is needed, starting from the thorough knowledge of factual reality – see, in this connection, the conference organised by the Garante on ‘Digital Borders: New Scenarios for Data Protection’, which was held on the occasion of the 2019 European data protection day and whose proceedings were published in a booklet available on the Authority’s website as web doc. No 9078052. In pursuing this new, rocky path one should recall the warning (and the incitement) given by Giovanni Buttarelli – who will always have a place in our hearts – first and foremost to the representatives of data protection authorities in his opening speech at the 40th international data protection conference (Debating Ethics: Dignity and Respect in a Data-Driven Life / Choose Humanity: Putting Dignity Back into Digital): ‘All revolutions have victims. So in the Fourth Industrial Revolution, who are the winners and losers? How can we develop a positive relationship with new technologies, which puts people and dignity at the centre? This is about defining the values of the future. And we have to do it before it is too late.’