GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ITALIAN SUPERVISORY AUTHORITY / GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

ANNUAL REPORT 2018 – EXECUTIVE SUMMARY

1.1. In a nutshell, one might argue that the 25th of May, 2018 – when the EU General Data Protection Regulation became applicable – marked a veritable watershed moment in terms of the activities carried out by the Italian supervisory authority in 2018 (Section IV, Table 1).

In the first part of the year, when the previous legal framework was applicable, several proceedings were finalised concerning, in particular, inspections and prior checking activities (paragraph 10.1 and paragraph 14.6); some of those proceedings allowed finalising pending complaints (Chapter 19) as regulated specifically by the national legislation. Such complaints proved to be especially effective to enforce the exercise of data subjects' rights throughout the past years of activity, and the relevant procedure was replaced by the more general 'complaint' procedure as set out in the GDPR (paragraph 5.4.1; see also Section 19(5) of legislative decree No. 101/2018). The legislative process intended to adapt the national legal system to the GDPR was monitored closely and in parallel by the Garante as well.

In the latter part of the year, the SA focused conversely on the new legal framework, in particular following entry into force of the national legislation enacted further to the GDPR – namely, legislative decree No. 101/2018 as mentioned above, which made substantial amendments to the so-called consolidated data protection code, i.e., legislative decree No. 196/2003. To a great extent, the work done was modelled after the one that had started in 2017 (see the 2017 Annual Report, p. 6 and ff.).

Whilst it could be argued that the main innovations brought about by the GDPR are, albeit substantial, in line with the preceding legislation – which was also grounded in EU law, i.e. in directive 95/46/EC – one cannot but highlight certain key changes. These include, first and foremost, the enhanced cooperation with the other EU supervisory authorities as laid down in Chapter VII of the GDPR – see paragraph 22.1; the amended rules applying to processing activities in the law enforcement sector, which have been taken out of the data protection Code as they are now regulated separately by legislative decree No. 51 of 18 May 2018 – transposing directive 2016/680 (paragraph 2.2.); the various tools – such as the data protection impact assessment, the appointment of a data protection officer, the implementation of certification mechanisms – introduced by the GDPR under the umbrella of the enhanced accountability all data controllers are expected to ensure, in that they are called upon to account for the technical and organisational measures they have put in place to achieve lawful processing activities along with respect for data subjects' fundamental rights; and the more effective sanctions envisaged against this background (see paragraph 21.7).

The complex management of this transition phase was actually compounded for the Italian SA by the new logistics arrangements following the move to its new offices in Piazza Venezia, in Rome, which took place at the end of 2018 (see Section III).

1.2. The past year marked a transition phase at supranational level as well (see Chapter 22). The modernization process concerning Council of Europe's Convention 108/81 was also completed, so that

the Amending Protocol to that Convention could be adopted on 18 May 2018; Italy signed the said Protocol on 5 March 2019. At EU level, the European Data Protection Board replaced the 'Article 29' Working Party seamlessly, even though organisational changes were made necessary on account of the different features of the Board - which has legal personality and is equipped with a Secretariat of its own. The new Board went on working to provide guidance on the implementation of the new legal framework grounded in the GDPR. In that respect, the Board endorsed the guidelines the 'Article 29' Working Party had been issuing on GDPR-related topics ever since 2017, whilst several public consultations were launched to gather inputs and suggestions on the adopted documents – with particular regard to new issues such as certifications, data protection impact assessments, and personal data breach notifications. As from 25 May 2018, the EU SAs also started cooperating under the terms of the GDPR to handle complaints and breaches related to cross-border processing activities. This is a revolutionary approach whereby the competent authorities from several Member States are called upon to jointly decide the cases having cross-border impact, also with the help of a shared IT platform (the so-called Internal Market Information System, IMI: see paragraph 14.8). To that end, they are expected to first exchange all the necessary information and carry out inspections, where appropriate also jointly.

1.3. Coming more specifically to the activities carried out by the Italian SA and following the above time sequence, one should point out that the first six months of the past year allowed significant decisions to be made with regard to the oversight tasks committed to the SA. Those decisions concerned, in part, sectors that had already been impacted by the SA with particular regard to telecom operators. In the latter sector, the decisions made by the SA concerned a substantial number of data subjects (up to several millions) mostly on account of breaches committed in connection with telemarketing-related processing activities (see paragraph 10.2). Accordingly, fines amounting to Euro 4,400,000 were imposed, of which Euro 3,800,000 could be levied in 2018 and the remainder was carried over to 2019 – out of a total of Euro 8,161,806 levied by the SA in 2018 (see paragraph 21.6.2). Other decisions concerned sectors that had been investigated to a lesser extent up to the past year, even though they are bound to take on a key role in the new legal framework as they involve major global players. Reference should be made in that regard to the decision that was adopted by the SA following the cooperative inquiries carried out with other EU SAs into a data breach that had taken place in 2016, but had been disclosed only in November 2017. The data breach had been caused by a hacking attack that had affected the data of tens of millions of customers worldwide of a multinational group; this group handles a well-known online platform that is intended to provide private transportation services via a mobile app connecting passengers and drivers directly (paragraph 15.1). In yet another case, the SA found that a well-known messaging service had unlawfully disclosed user data to the leading social networking platform (paragraph 11.1).

Regarding other areas of the SA's activity, prior checking requests rose to 37 in the first six months of 2018, compared to 26 throughout 2017; prior checking was regulated by Section 17 of legislative decree No. 196/2003 and several controllers relied on this tool which is no longer applicable following entry into force of the GDPR – indeed, it is now superseded by the data protection impact assessment as provided for in Article 35 of the GDPR. The latter circumstance had been pointed out by the SA in connection with a prior checking request concerning the proposed surveillance of vehicles intended for the transportation of disabled individuals as well as of the individuals themselves – see paragraphs 5.4.2 and 13.2. On top of the sectors considered in the past years – see paragraph 10.1 on processing activities carried out for marketing and profiling purposes in connection with purchasing semi-durable goods – those prior checking activities allowed addressing increasingly sophisticated types of processing: from 'wearable' image recording systems (paragraph 13.4) to smart video surveillance (paragraph 14.4.), partly with a

view to the enhanced automation of highway toll payments (paragraph 14.5), up to the growing use of biometrics also by the police (paragraph 7.2). The SA's assessment focused increasingly on the localization of individuals by way of ad-hoc sensors that could be traced back to those individuals, whether directly or not. The SA found that the processing activities in question were lawful, in principle, but set forth measures to protect the rights and dignity of the individuals concerned – including non-autonomous patients wearing localization bracelets or anklets (paragraph 5.1) or employees, whose activities can be indirectly (and pervasively) monitored by way of the devices committed to them (vehicles, smartphones, tablets, etc.) in both the private (paragraph 13.3) and the public (paragraphs 13.7 and 13.9) sector.

1.4. The latter part of the year featured, in particular, increased work to bring the SA's operational mechanisms fully in line with the new legal framework.
The so-called 'general authorisations' applying to the processing of 'sensitive' data were revised pursuant to Section 21 of legislative decree No. 101/18, so that the provisions contained in those authorisations that were compatible with the GDPR could be identified by a decision dated 13 December 2018 – on which a public consultation was launched on 11 January 2019 via a notice published in Italy's official journal (see paragraph 5.4.4). Under the terms of Section 20(3) and (4) of the said legislative decree No. 101/2018, the SA assessed to what extent the provisions set out in some of the 'Codes of practice and conduct' attached to the data protection Code were compatible with the GDPR (in particular, the codes contained in Annexes A2, A3, and A4 to the Code). The compatible provisions were grouped into 'Rules of conduct' and attached to the amended data protection Code (Annex A) – see paragraph 5.4.4. This exercise was also carried out with regard to the 'Code of practice applying to the processing of personal data in connection with journalistic activities', leading to the adoption of 'Rules of conduct applying to the processing of personal data in connection with journalistic activities' (Chapter 8). The multi-step revision process concerning other codes of practice and conduct (as contained in Annexes A.5 and A.7 to the former data protection Code) was also started pursuant to Section 20(1) of legislative decree No. 101/2018 (see paragraph 14.3).
Furthermore, a non-exhaustive list of cross-border processing activities subject to mandatory data protection impact assessment was also set out (see decision No. 467 of 11 October 2018), without prejudice to the guidance provided by the 'Article 29' Working Party in the 'Guidelines on data protection impact assessment' as last revised on 4 October 2017 and endorsed by the European Data Protection Board on 25 May 2018 (WP248, rev. 01).
Further clarification was provided concerning qualifications and activities of data protection officers, following the initiatives that had been implemented in 2017 – by way of ad-hoc meetings involving both public sector and private sector stakeholders (see paragraphs 5.4.3 and 14.1, respectively) and within the framework of wider-range initiatives (see paragraph 24.4).

1.5. Striking the right balance between transparency and personal data protection remains one of the topmost commitments for the Italian SA. This is shown by the many opinions rendered on FOIA-type access requests to Transparency and Anti-Corruption Officers as well as to Ombudspersons (paragraph 4.2.1). Indeed, the SA itself received several FOIA-type access requests throughout 2018 (paragraph 26.4).
Reference should be made in this respect to the recent judgment by Italy's Constitutional Court (No. 20 of 23 January 2019), whereby Section 14(1-a) of legislative decree No. 33 of 14 March 2013 was found to be unconstitutional because in breach of reasonableness and equality principles. The said decree regulates FOIA-type access rights and the transparency, publicity, and disclosure obligations applying to

public administrative bodies. The provisions at issue envisage that public administrative bodies must publish the information referred to in Section 14(1), letter f), of the decree with regard to all senior officials – i.e., a statement concerning rights in rem on immovable property and registered movable property, any stock or corporate interests held, and any positions covered as members of the board of directors or auditors for any company along with a copy of the latest income statement. This requirement also applies to unseparated spouses and second-degree relatives subject to their consent, whereby non-consent must be documented. When commenting this judgment, the President of the Italian SA remarked that it 'clearly points to a good practice in reconciling personal data protection and other interests as protected by the Constitution, whenever such interests happen to be in conflict with the former as part of public policies'. The President of the SA also criticised certain legislative measures, whether recent or not, which feature 'some scoffing' at the SA's call for 'respect of the proportionality principle, which must underlie any balancing between rights, freedoms and other primary goods'; he hoped that 'additional care' would be taken in future 'following the lead of the Court, in line with the reasonableness principle'. The same considerations had actually been made in the past exactly regarding transparency legislation (see the 2013 Annual Report, p. 27 and ff., and the 2016 Annual Report, p. 15 and ff.) as well as in respect of other items of draft legislation that envisaged the centralised collection of personal data – in some cases involving the whole of Italy's population and affecting the most intimate sphere of one's life. This is the case, in particular, of the 'National Data Platform' (see the 2017 Annual Report, p. 37, on which the SA's concerns were reiterated in a decision dated 22 May 2018, No. 31) as well as of the processing operations performed by Italy's National Statistics Institute (ISTAT) (see the 2017 Annual Report, p. 71; the issue is mentioned in paragraph 6.2 of this year's Annual Report).

1.6. Those concerns continued in the first months of 2019, indeed additional concerns were raised in connection with implementation of blanket electronic invoicing (e-invoicing) obligations – see paragraph 4.5.2 for further details. Reference should also be made to the call recently made upon Parliament to ensure respect for the proportionality principle - for instance, in the brief submitted by the President of the SA with regard to the bill intended to enact decree-law No. 4 of 28 January 2019, which contained urgent measures on introducing the universal basic income and regulating retirement benefits. The brief was submitted on 8 February 2019 to the XI permanent committee of the Senate; an additional brief was lodged on 6 March 2019 with the joint XI and XII committees of the Chamber of Deputies, taking note of the amendments made – as requested - in the enactment process of the said decree-law. The same call for proportionality was made by the President of the SA during the public hearing held on 6 February 2019 before the joint I and XI committees of the Chamber of Deputies, in connection with the bill containing measures to ensure effectiveness of public administrative activities and to prevent absenteeism.

Once again, it is the pillars of personal data protection that are impacted, which is not infrequently accounted for by the alleged need to achieve effectiveness of administrative activities. Those pillars are made up by the principles of relevance and proportionality along with the purpose limitation principle - as recalled of late by the Constitutional Court and set forth in Council of Europe's Convention 108 already prior to being enshrined in EU-related legislation. This is why one cannot but welcome the innovation brought about by Article 36(4) of the GDPR and hope that it will bear its fruits – namely, the obligation to consult the supervisory authority 'during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing'. Indeed, this exercise has already been carried out successfully at domestic level several times over the past years in terms of the relationships between the SA, Parliament and the Government. The underlying rationale is to consider the Italian SA a fundamental institutional partner in

order to make sure that the modernisation of Italy as based on an enhanced digital infrastructure can take place in full compliance with personal rights and fundamental freedoms.