HIGHLIGHTS – ANNUAL REPORT 2017
Garante per la protezione dei dati personali

January

We tackled, once again, unsolicited marketing calls and prohibited an IT services company from using phone numbers collected on the Internet – usually by searching for phone numbers of professionals and single-person companies as available in the 'Contacts' section of the individual websites. We found this processing to be in breach of the purpose limitation principle and to be carried out without the data subjects' informed consent. Contact information available on the Internet, though accessible to everyone, may not be used for whatever purposes; in the case at issue, that information was intended to facilitate the professional activities of the individuals concerned [par. 10.3]

.....

Taking account of the activities involved, we authorised the processing of judicial data, with particular regard to data concerning offences against property and the State's personality, as related to specific professionals working for a company that also provides its services to institutional entities in highly strategic areas for our country [par. 13.6]

.....

Several inspections were carried out throughout the year both in Italy and abroad (in cooperation with the Albanian supervisory authority) to counter the so-called wild telemarketing as benefiting, in particular, telephone and utility companies. Several decisions were adopted in 2017 (and in early 2018) establishing (and partly imposing fines for) millions of unlawful calls; detailed measures were ordered to be taken in that respect [parr. 10.2 and 10.3]

February

Starting from February, we rendered several opinions on the multifarious cases submitted to our attention by anti-corruption officers and ombudspersons (pursuant to Section 5, paragraphs 7-8, of legislative decree No. 33/2013) to provide guidance to public administrative bodies on whether to grant FOIA access requests under Section 5(2a), letter a), of legislative decree No. 33/2013 if this could factually affect personal data protection rights [par. 4.3.1]

.....

A complex opinion was rendered to the Ministry for Home Affairs on the draft decree setting out – pursuant to Section 53(2) of Italy's DP Code – the non-occasional processing activities of personal data as carried out with electronic tools for police purposes at the Data Processing Centre of the Public Security Department, or else by public security and other public bodies acting on the basis of the authority conferred on them by laws or regulations. The decree will have to be published on the Official Journal and appended to the DP Code as Annex C. [par. 7.3]

.....

As part of an investigation carried out by Rome's Prosecuting Office and with regard to the breaches of administrative law established in that context, we imposed fines totalling over 11 million euro on five money transfer companies that had processed the personal data of over one thousand individuals unlawfully and without their knowledge. The personal data of those individuals were used unlawfully via the split payment technique to transfer, to China, sums that could be traced back to Chinese entrepreneurs [par. 21.5.2]

March

We rendered our opinion on a draft Presidential decree pursuant to Section 57 of the DP Code, setting out the arrangements to implement the principles of the DP Code in connection with processing of personal data by the police for preventing and suppressing criminal offences and protecting public order and security. The draft decree had already taken on board many requests made by our DPA in the preparatory phase. In our opinion, we requested the Ministry to expand the scope of protection by including processing activities that feature specific risks to individuals (databases including genetic or biometric information and/or location data, databases relying on specific information processing techniques, etc.) as well as to lay down shorter data retention periods that would be proportionate to the purposes of data collection [par. 7.3]

.....

Further to a prior checking application lodged by a water utility company in respect of the processing of their fleet location data for several purposes, we established that the geolocation system in question might enable the remote surveillance of employees and decided that its

deployment required a prior agreement with trade unions or, failing this, an authorisation by the national labour inspectorate – in spite of the changes made to the applicable legislation under the so-called Jobs Act. Additionally, we required the company to provide full information to employees and set out the arrangements to collect, process and store geolocation and other personal data by envisaging different safeguards in the light of the specific purpose to be achieved. Finally, we ruled out any monitoring of fleet routes, except for processing the relevant data in aggregate or anonymous format for the purposes of statistics and work planning [par. 13.2]

.....

We rendered the required opinion on the draft of the latest inter-ministerial decree regulating operation of the DNA database, which deals with the arrangements for erasing, entering, destroying and storing DNA profiles. In that connection, we requested genetic information and other personal data in the database to be updated continuously also in the light of the outcome of judicial proceedings rather than at pre-defined intervals, so as to ensure fair processing. In particular, we requested timely erasure of the data relating to individuals who have been acquitted of the charges brought against them via a final judgment – on whatever grounds: because there is no case to answer, the defendant is found not to have committed the offence, the facts of the case do not amount to a criminal offence, or the facts of the case are not classed as a criminal offence under the law. We also highlighted the importance of adequately informing each individual whose profile is stored in the database along with the need to clarify the rules mandating erasure of a DNA profile and to better detail the entities authorised at domestic level to access these highly sensitive pieces of information [par. 7.4]

.....

We rendered a favourable opinion on the draft regulations concerning operation of the Cancer Registry for Latium Region, which sets out the categories of sensitive data, the processing activities that may be performed and the specific purposes sought by the Registry along with the entities authorised to access it and the data security measures. Most of our recommendations had already been taken up in the preparatory stage; they were intended to ensure high security standards, clear-cut specification of the purposes to be achieved as well as compliance with the data minimization and necessity principles. The draft leaves some room for improvement especially in terms of limiting the scope of the processing to what is really necessary as well as in terms of security measures [par. 6.1]

April

In-depth investigations into a data breach case were sparked by a detailed complaint whereby a user reported the unjustified activation under his name and without his knowledge of a substantial number of telephone landlines (over 800) by a major telephone services provider. We could establish that this misallocation was due to mistakes made during a massive migration of customer data to the new CRM system and had involved a considerable number of customers over a long period. We stigmatised the negligence and inaction showed by the data controller, who had failed to carry out the required checks over a long time span even after being notified of the misallocations in question and had thus breached the fair processing principle – whilst by acting otherwise it could have made available remedies firstly to the complainant, and secondly to all the subscribers happening to be in a similar situation. Furthermore, we ordered the controller to take detailed measures and monitored that those measures were implemented, and we also served the controller with an enforcement notice for the fines due on account of the violations established as above [par. 11.3]

.....

We rejected the application lodged by a company specialising in auto glass repair and replacement to have a balancing of interests decision issued in their favour so as to set up a database collecting information to check possibly fraudulent activities in the insurance sector without the data subjects' consent. The prevention of and fight against fraud are regulated by laws that entrust management of the databases set up for those purposes to public bodies ensuring the required impartiality – which was not the case of the company in question [par. 14.2.2]

May

The processing of data performed whenever the 'Multiservice Card' of the Defence Ministry is issued/renewed was found to be unlawful by our DPA. Accordingly, we ordered the issuance

process of those cards to be modified by banning the processing of biometric data that had been stored in breach of the applicable legislation. We highlighted that the application of certain Sections in the DP Code was only ruled out if the processing was carried out for purposes related to State defence or security as based on specific provisions in laws that expressly refer to such processing. For the remainder, processing of fingerprint data is only allowed following the green light given by the DPA on the basis of a prior checking application [par. 13.5]

……

Starting in May this year, we launched awareness-raising and outreach initiatives vis-à-vis the public and private sectors spanning the whole period till the date of full application of the General Data Protection Regulation (GDPR), on 25 May 2018. [parr. 1.10, 1.11 and 23.1]

June

We rejected the application lodged by a company to be authorised to process employees' judicial data by collecting and processing the respective criminal records in order to comply with a clause in a procurement contract whereby the client was to be informed timely of any employees with records of final criminal convictions as well as of the specific criminal offences and the sentences imposed. We reiterated that an employer may only process judicial data if an appropriate legal basis exists whether in a law, regulation or contractual instrument [par. 13.6]

……

Further to complaints and on-the-spot inspections, we established the unlawful processing of the data contained in a large database used for telemarketing purposes in the dental medicine sector. Such database had been purchased by the controller from a mailing list provider established outside Italy [par. 10.3]

July

We rendered the required opinions concerning the 'APE' (pension advance payment) legislation; we provided guidance on the information to be provided to data subjects, the roles played by the individual stakeholders in processing data and the measures required to ensure minimization of the data contained in email communications. We also advised on the draft Framework Agreement for the APE and the Framework Agreement on compulsory insurance for early death, which are to be entered into between the Ministry of Economy and Finance and the Ministry of Labour and Welfare, ABI [Italy's Banks Association] and ANIA [Italy's Association of Insurance Companies] [par. 4.8]

……

We gave a favourable opinion on the draft Presidential decree concerning collection, access to, communication, erasure and updating of the data stored in the Data Processing Centre (CED) of the Police. Along with the opinions rendered in February and March, this opinion finalised the regulatory process regarding the personal data processed for police purposes and enabled accordingly full implementation of the provisions set out in Title II of Part II of the DP Code. The draft decree took on board the guidance provided by the DPA in the course of several meetings aimed at bringing the draft fully into line with data protection legislation. The decree now provides for the appointment of a data protection officer in charge of awareness-raising and supervision and also sets out the rules on data storage and disclosure. It was considered appropriate for the specific security measures to be detailed in a separate regulatory instrument, whilst we banned any bulk extraction or copy of the information pooled into the CED [par. 7.3]

……

We handled all the reports we received in connection with cyberbullying, pursuant to the timeline set out in Law No. 71 of 29 May 2017 (for the protection of children and the prevention of and fight against cyberbullying). The reports in question concerned the creation of fake profiles - at times for the purpose of exchanging sexually-oriented messages – and the dissemination of abusive messages and/or pictures taken in a private context; to protect data subjects, we contacted social media and website managers both in the EU and in third countries [Chap. 9]

September

To enable compliance with vaccination obligations in accordance with the tight schedule envisaged in the law, we issued an urgent decision – made necessary by the impending start of the school year – to authorise schools to communicate non-sensitive personal data to health care authorities. This enabled data processing operations that would actually only be permitted as from 2019 based on the applicable vaccination laws [par. 5.2.1]

We established the unlawful processing of email addresses taken from social networks for marketing purposes (so-called social spam), failing the required documentation of the data subjects' informed consent. We banned any further processing of the data and reserved the right to serve an enforcement notice on the controller, whilst reiterating that the mere subscription to a social network does not legitimize the processing for marketing purposes of any data provided to that social network by other subscribers [par. 10.4]

October

We rendered a favourable opinion on the draft legislative decree amending the Digital Administration Code and provided some advice to further bring its contents into line with personal data protection legislation [parr. 2.1.2]. We drew the Prime Minister's attention to our criticisms concerning the proposed creation of a National Digital Data Platform on the basis of a Section that had been added to the Code without requesting the Garante's opinion beforehand; management of the platform would be committed initially to the Extraordinary Commissioner in charge of implementing the 'digital agenda'. The platform would pool and duplicate all the data held by public administrative bodies for purposes that are as yet quite unclear [par. 4.2]

Taking account of the many requests for clarifying provisions contained in the Code of Conduct for Credit Bureaus and in accordance with the most recent decisions by Italy's Court of Cassation, we clarified the following: a creditor must provide proof that the data subject has received the advance notice of inclusion in the relevant Credit Bureau database; the maximum retention period should not be in excess of five years after expiry of the contractual relationship, in case of payment defaults that have not been remedied; when drafting the SECCI customised information notice one should only take account of the information made available by the consumer and may not access credit bureau data, as the provisions set out in the Code of Conduct only apply if a loan application/contract exists and should not be invoked prior to the filing by a consumer of a loan application as such [14.2.1]

November

We found that the processing of employees' personal data as performed by a postal services company was unlawful and accordingly banned it by having regard to the newly introduced queue management system. The preparatory inquiries showed that the monitoring dashboard used by the company to that end enabled over 12,000 individuals tasked with the relevant processing to access, in real time and on a permanent basis, the data from all workstations – albeit with different degrees of visibility between central and peripheral operators. The processing operations resulting from this system were accordingly in breach of data minimization, necessity and relevance principles by having regard to the purposes to be achieved; additionally, the processing was in breach of the sector-specific legislation on remote surveillance of employees [par. 13.3]

Taking account of the peculiarities of the industry sector in question as well as of the substantial risks run by car rental companies, we granted a prior checking request concerning the processing of personal data for setting up a database that would only be used to check against customers who, over a given time span and on whatever grounds, had failed to return rented vehicles. Access to the database will be granted only following an official car rental request [par. 14.2.2]

December

Following a prior checking request, we considered it lawful – subject to compliance with specific conditions – the processing performed by way of advertising totems equipped with image detection devices that allowed processing the collected data to assess the ad audience. It was clarified in this connection that the system only enabled detecting the presence of human faces without identifying the individuals via biometrics, and that the images would be stored only locally and temporarily and would be overwritten by subsequent images [par. 14.3]

Given the persistent availability on the web of contents producing a 'disproportionately negative' effect on the private sphere of a complainant domiciled outside the EU – partly on account of the processing of potentially sensitive information concerning that complainant – we

ordered a major search engine to de-index all the URLs under the complainant's name in both EU and non-EU versions (i.e. to implement the so-called global de-indexing) [par. 19.3]

……

We rendered a favourable opinion on the draft Presidential decree amending the legislation on the Public Opt-Out Register as submitted by the Ministry of Economic Development. Under the decree, the relevant regulations will also apply to conventional mail as for the processing of personal data in mail addresses. We pointed out, among other things, the advisability of waging campaigns to raise awareness of the amendments made and recommended introducing a transitional regime whereby data subjects would be able to opt out of the use of their addresses as contained in public lists or records [par. 10.2]

_____