GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

ITALIAN DATA PROTECTION AUTHORITY

ANNUAL REPORT FOR THE YEAR 2015 // HIGHLIGHTS

JANUARY

Following a request made by the National Alpine Rescue Corps, we decided geolocation systems could be lawfully used to locate individuals gone missing in mountain areas via their smartphones; we made this conditional upon ensuring that the collected data should only concern the geographic location of smartphones and be used to protect the individuals' lives or bodily integrity.

We banned further dissemination of data suitable for disclosing health via the website of a Region; the data concerned participants in a public event intended for disabled individuals. We also ordered that Region to remove web copies of the data from search engine lists and cache memories.

We decided against the processing performed by a local police consortium, which relied on video surveillance systems deployed on their car fleet plus geolocation of the palmtop devices provided to their employees. We banned location-based processing, which ultimately enabled all the operators to access several data items relating to their colleagues, because it was excessive and unnecessary for the purposes at issue as well as being in conflict with the safeguards set forth in Italy's law on workplace rights ('Statuto dei lavoratori').

FEBRUARY

We found that the processing of personal data related to the browsing of the Internet by the employees of a marketing communications company was unlawful and accordingly prohibited the company from continuing that processing. Network traffic was monitored without informing employees and in the absence of a policy setting out the standards for employees' use of electronic devices; the monitoring allowed the employer to track down who was using which device.

On the occasion of a study visit by a delegation of the Albanian data protection authority, a Cooperation Agreement was signed partly to facilitate joint inspections into telemarketing activities by call centres.

We gave a favourable opinion on the draft decree by the Director of the Revenue Agency setting forth the technical arrangements for taxpayers and other authorised entities to access the tax return forms ('730 forms') made available by the Agency; the decree took account of the guidance provided by the Authority to prevent unauthorised access to taxpayers' data.

MARCH

We launched a public consultation on the 'Internet of Things' (IoT) to gather suggestions and proposals on data protection issues with regard to the interaction and interlinking of networked things and devices; this was aimed ultimately to develop guidance enabling users to stay in control of their data.

We requested the Ministry of Health to make certain amendments to a draft Regulation on the procedures for the nationwide interlinking of information systems held by the National Health Service; the requested amendments – including enhanced safeguards to be implemented in the information system for hospital discharge forms and stronger data access security measures – were a precondition for the Authority to give a favourable opinion on the draft.

To harmonize and simplify online profiling activities and provide better safeguards to users, we spelled out the rules to be followed by online service providers in ad-hoc Guidelines. Those rules include, in particular, the obligation to obtain informed consent from both authenticated and non-authenticated users, who may withdraw their consent at any time, and to provide adequate information notices.

We prohibited a Region from further disseminating the personal data contained in a resolution that had been posted on the online billboard for longer than permitted under the law. The data consisted in assessments of an employee's professional conduct and had resulted in the employee's removal to a different office.

APRIL

We gave a favourable opinion on a draft decree concerning the so-called 'expanded newborn screening' (ENS) for the early diagnosis of inherited metabolic diseases; however, we requested additional safeguards to be built in as for the parents' informed consent and the information notice – which must highlight whether providing the data is mandatory or optional, what medical treatment and genetic advisory purposes are aimed at, and what is the scope of data communication. The consent form will have to include the statement, if any, whereby the parents accept to be informed of the outcomes of such screening.

We gave a favourable opinion on a draft legislative decree transposing Directive 2013/37/EU of 26 June 2013 on the reuse of public sector information. The draft decree had taken on board the indications provided by the DPA as for the reuse of any document in which intellectual property rights are owned by libraries, museums and archives; the limitations placed on accessing documents that contain non-publicly available personal information; and the use of open licences as available online.

MAY

We ordered Sky Italia S.r.l. to make access to the contents of a reminder for arrears – sent to customers' decoders in the form of a banner displaying the icon of an envelope – conditional upon entering a personal code. We considered that customers would be exposed otherwise to the risk of unlawful dissemination of information related to their defaults.

We gave a favourable opinion on a draft decree by the Ministry of Education, University and Research regulating the deployment and delivery of personalised student cards called 'IoStudio', which are meant to enable the holders to access cultural services and utilities at reduced costs and can also work – on request – as anonymous debit cards. We established that only indispensable information would be used, that such information would be deleted upon expiry of the initiative, and that the students would be provided with the relevant information when registering online for their first high school year.

We requested certain conditions to be fulfilled before giving our favourable opinion on a draft decree by the Ministry of Economy and Finance regarding technical and operational rules for the network-based handling of tax claims. Those conditions related mostly to the mechanisms for identifying the entities authorised to access the Information System of the authorities handling tax claims ('giustizia tributaria'), to logging of the accesses to computerised case files, and to the procedures for including files and records into the general registry.

On the occasion of the 2015 Sweep Day, which focused on the protection of children aged 8 to 13 surfing the Web, we found substantial criticalities among the apps and websites taken into consideration; they had to do mostly with poor transparency in the collection and use of personal data, the mechanisms for requesting authorisations, advertising and the risks that children might be routed towards unsafe sites.

JUNE

We adopted new Guidelines on the electronic health dossier to provide a unified reference framework when processing data in this sector as well as to afford enhanced safeguards and top-level security standards to patients. More specifically, data controllers were required to notify the DPA of any personal data breaches and patients were found to have the right to view the access logs relating to their health dossiers.

We gave a favourable opinion on draft Guidelines explaining how to have one's acceptance or refusal to donate organs or tissues noted in one's ID. All of the suggestions made by the DPA were taken on board; they concerned mechanisms to inform data subjects, the possibility to change one's mind at any time and have the relevant choice noted in the ID, the rights granted by the Data Protection Code and the data exchange arrangements between municipalities and the 'Transplantation Information System' (*Sistema informativo trapianti, SIT*).

We authorised Bank of Italy – in compliance with the DPA's general authorisation 7/2014 – to process judicial data relating to external collaborators that access specific, 'security-sensitive' areas as part of their tasks; the processing in question was aimed at performing *ex ante* controls on criminal records and pending criminal proceedings in respect of those collaborators.

We called for enhanced safeguards to ensure workplace privacy in the opinion we gave on the draft inter-ministerial decree submitted by the Ministry of Labour and Welfare setting forth technical mechanisms for the issuance of medical certifications of pregnancy, abortion and childbirth, which are to be sent by law to the national social security agency (INPS). The safeguards concerned, in particular, the electronic transmission of such certificates at the worker's request, suitable security measures and the data to be included in the certificates.

We ordered a company to immediately terminate the processing of personal data relating to Skype-based conversations between an employee and third parties, as this was found to be in breach of the laws protecting confidentiality of communications as well as of the Guidelines issued by the DPA in 2007 and the company's own privacy policy.

We gave opinions on two draft measures by AGID [Italy's Agency for Digitalisation] – namely, a draft regulation with implementing arrangements for the SPID (the public system managing the digital identities of citizens and undertakings) and a draft regulation containing the relevant technical requirements. These topics were addressed in 2015 as also related to the procedures to be followed by the accredited entities in issuing digital identities and with regard to the agreements to be entered into by AGID and the said entities. The drafts were found to be compliant with most of the indications given by the DPA as part of an ad-hoc technical working group; however, we requested additional specifications to be made in order to better protect data subjects such as by introducing enhanced security standards for digital identities.

JULY

We laid down stringent rules for the interlinking of public bodies' databases including the obligation to notify the DPA of any potentially significant data breaches or IT incidents within 48 hours of their becoming known.

We required IVASS [Italy's Supervisory Body on Insurance Activities] to amend a draft regulation and a decision related to such regulation concerning the database of (insurance) risk profiles as a precondition to obtain our favourable opinion. The amendments focused on clarifying the purposes sought by way of the transmitted information, security measures, and information and consent mechanisms; additionally, we requested IVASS to specify the maximum storage period of the information contained in the database.

We gave a favourable opinion on a draft decree by the Ministry of Economy and Finance as well as on an accompanying draft decision by the Head of the Revenue Agency. In compliance with the guidance provided by our DPA, those two instruments set forth the mechanisms for electronically transmitting health expenditure data to the so-called 'Health Card System' - with a view to compiling the tax return form - and the corresponding user technical specifications, respectively.

In order to give a favourable opinion on a draft decree by the Prime Minister's Office regarding surveillance systems and registries of mortality, cancer and other diseases, we requested that the draft be amended by adding certain provisions. The latter concerned, in particular, the mechanism to verify that the appropriate conditions were fulfilled to allow using the data for treatment purposes, the implementation of specific data protection precautions, and the obligation for data controllers to timely inform the DPA of any data breaches.

SEPTEMBER

After analysing the contributions received via a public consultation, we approved the 'Code of Conduct on Business Information Systems'. The Code is aimed at laying down rules on the appropriate use of business reliability information with particular regard to the reports containing information on entrepreneurs and managers.

A public consultation was launched on a draft general scope decision concerning the processing of personal data in connection with mobile ticketing; the consultation was aimed at gathering inputs to develop a coherent set of measures to protect users and ensure the appropriate handling of personal information in this context.

We banned further dissemination of decisions awarding allowances to mentally impaired individuals that had been posted on the website of a health care agency, since those decisions contained data suitable for disclosing the individuals' health as well as excessive information.

OCTOBER

Taking account of the contributions from both the public consultation launched in 2014 and the stakeholder meetings we had organised thereafter, we found it admissible to set up the so-called 'SIMOITEL' – i.e., an information system on intentional defaults in the telephony sector. The defaults in question are not due to transient payment difficulties, but to users' specific decisions; as such, they do not include defaults of a temporary nature caused by lack of experience, forgetfulness or money problems.

We banned a correctional institution from further processing, for disciplinary purposes, biological samples taken from the inmates along with the respective laboratory reports as such processing was found to be in breach of the law.

We prohibited processing operations related to marketing calls that were made by a call centre on behalf of a telephone company without the users' prior consent, as those users were not listed in public directories and were thus unable to rely on the opt-out register.

We ordered a health care agency to enrich the information notice and take appropriate measures to ensure that the staff would only access the health dossiers of the patients undergoing treatment for no longer than the duration of such treatment. This was aimed at preventing unauthorised accesses to patients' data and remedying serious breaches that had been detected in the course of inspections.

We gave a favourable opinion on a draft regulation by the Ministry of Education and Universities on the processing of data relating to students with disabilities as included in the National Students' Register; our green light was made conditional upon the definition of a suitable, proportionate storage period for the access logs. In order to enhance confidentiality, especially sensitive information such as disability certificates, functional diagnoses, dynamic-functional profiles and customised educational programmes will have to be included in a separate section of the Register after removing the students' names.

NOVEMBER

After the prior checking performed at the request of Consiglio Nazionale del Notariato [National Council of Notaries Public], we authorised the deployment of a graphometric signature system that was considered capable to enhance authenticity and integrity of electronically signed documents and records.

We required several measures to be taken as a precondition to give our favourable opinion on a draft regulation by the Ministry of Justice that set out the arrangements for electronically registering last wills and testaments in the respective General Register. Those measures included enhanced security requirements and the introduction of more detailed provisions on the transmission and storage of IT documents and records - given the confidentiality and secrecy constraints applying to the information at issue.

DECEMBER

We ordered a health care agency to discontinue the dissemination of personal data relating to the users that had registered on the agency's website, in order to prevent unauthorised accesses. The users' data could be retrieved and modified quite easily thanks to a search function made available on the website in question.

We found that the processing of personal data carried out in the course of a well-known radio show was unlawful because of the specific mechanisms – in particular, statements were obtained and then broadcast from individuals that had been contacted on the phone by speakers assuming fake identities.

Regarding the automatic mandatory exchanges of tax-related information and pursuant to two opinions given by the DPA in July on the FATCA Agreement – which is intended to improve international compliance in taxation matters – we gave a favourable opinion on a decree by the Ministry of Economy and Finance that set forth the technical rules to collect, transmit and notify the Revenue Agency of any information on non-nationals in accordance with applicable international agreements.