ITALIAN DATA PROTECTION AUTHORITY
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

ANNUAL REPORT – 2013

Data Protection: Times Are A-Changing
Big Data, Transparency, Surveillance

HIGHLIGHTS

JANUARY

The DPA ordered appropriate arrangements to be made, also of a technical nature, to ensure that the information contained in health care records would only be accessible to the practitioner and/or the facility where such records were created and could only be shared with other practitioners treating a data subject at other medical units or wards with the data subject's specific consent – which may also apply to medical information relating to past clinical events.

The DPA prohibited the processing of data via a video surveillance system installed at a department store because it was in breach of data protection legislation as well as of the ban on employees' surveillance; furthermore, the security company tasked with managing the system to prevent robberies and shoplifting had not been granted the necessary authorization by the governmental *prefect* .

FEBRUARY

On the occasion of the 2013 European Privacy Day, cyberbullying was the focus of attention by the DPA. A video was posted on the DPA's website containing tips for the knowledgeable use of social networks and a letter was sent to the Ministry of Education to draw his attention regarding this sensitive issue.

The DPA gave a favourable opinion on the draft legislative decree by the Ministry for public administration and simplification concerning transparency obligations of public administrative bodies; however, several criticalities were pointed out by having also regard to EU law and guidance was provided to make sure that transparency would not be in conflict with the right to privacy and data protection – for instance, by preventing dissemination of information on health or economically or socially disadvantaged beneficiaries of public allowances.

The DPA prohibited several municipalities from posting, on their official websites, decrees on the enforcement of mandatory medical treatments.

To further counter "unregulated" telemarketing and unsolicited marketing, the DPA carried out several inspections and issued injunctions against two major IT companies specializing in database services, which had to pay hefty fines as they had failed to comply with orders the DPA had already issued in their regard.

MARCH

The DPA rendered an opinion to the Ministry of Economy and Finance on a draft ministerial decree regarding operation of the public system for the administrative prevention of consumer credit fraud, with particular regard to identity theft. As well as requesting compliance with purpose limitation requirements and the adoption of adequate security measures, the DPA found it necessary to include, in the relevant regulations, specifications on the different access arrangements applying to "direct" and "indirect" participants; furthermore, the DPA suggested including measures to inform data subjects of any data inconsistencies as found in the public databases following the checks to be performed.

With the help of the Financial Police, the DPA performed inspections on 11 telephone companies and ISPs to verify compliance with the legislation on Internet and telephone traffic data retention; the sanctions envisaged in the Code in case of non-compliance with previous orders by the DPA were also imposed.

To prevent the patients concerned from being identified, also indirectly, the DPA requested that aggregate data be used as part of the opinion rendered on the draft agreement between Government, Regions and the Trento and Bozen Autonomous Provinces concerning the guidelines for the assessment of the use of human cells and tissues (corneas, skin, heart valves) for experimental transplantations and new advanced drug therapies.

APRIL

A decision was adopted in pursuance of the legislation on personal data breach notification to provide guidance on who was required to fulfil the relevant obligations, what measures could ensure minimum common security standards, the timeline and contents of the notification – which may also be given via an ad-hoc downloadable form on the DPA's website.

MAY

The DPA required health care districts that had installed video surveillance equipment in the restrooms of the respective facilities for ruling out drug addiction cases to take measures and precautions such as to protect the privacy of any individual whose urine sample was being taken – in particular, the DPA banned the recording of CCTV images by whatever means.

The DPA found that the use of biometrics to check attendance of teachers and administrative staff in some schools was disproportionate.

With a view to simplification, it was clarified that a data controller obtaining data subjects' consent for direct marketing purposes via automated mechanisms may process the relevant data also according to conventional mechanisms (correspondence, operator-assisted phone calls) unless the data subjects object to the processing.

A Vademecum was drafted called "Privacy: Working with Business – Ten Corporate Best Practices to Improve Your Business", including some key practical indications to ensure compliance with personal data protection rules.

The use of webcams in a nursery school was banned by the DPA to protect children's privacy, the unfettered development of their personality as well as unrestrained relationships with their teachers and freedom of teaching.

JUNE

The police were prohibited from processing images captured via surveillance cameras that had been installed in a street for public safety purposes and allowed viewing inside people's homes.

JULY

The DPA required – and informed Regions, Autonomous Provinces and INPS [the national social security agency] accordingly – that the competent medical boards do not include the patient's clinical history, medical findings and diagnosis when issuing a copy of the invalidity certification that is to be submitted under the law in order to obtain, for instance, the car pass for restricted access areas or the tax deductions granted when purchasing motor vehicles.

Guidelines were adopted on marketing and for countering spam; special emphasis was put by the DPA on the new frontiers of spamming such as social spam (via SNS) or spam based on the so-called viral (or targeted) marketing, which may give rise to subtler, more pervasive interferences with a person's private life. An information page was published on the DPA's website (called "Spam: How You Can Defend Yourself") and a video tutorial was posted on the DPA's YouTube page.

Physical and IT measures and arrangements were laid down to foster the security of any personal data that is collected and used as part of the interception activities carried out by the Centri Intercettazioni Telecomunicazioni (C.I.T. – Telecommunications Interception Centres), which are attached to each prosecuting office in Italy as well as to police offices tasked with performing interceptions for judicial authorities.

SEPTEMBER

The DPA allowed two banks to equip their financial promoters with tablets that could perform the graphometric analysis of the signature affixed by any customer entering into financial agreements in electronic format; at the same time, the companies involved in enabling and managing both systems were required to take special measures to protect the data they collected along with measures to afford bank customers the option to undersign such agreements via conventional mechanisms as well.

OCTOBER

The DPA sent a letter to the Prime Minister urging him to support, within the EU Council, the adoption of the draft reform of the European regulatory framework on the protection of personal data by strengthening its overall rationale. The DPA voiced its concerns for the espionage performed by the NSA on telephone and Internet communications also relating to Italian citizens.

Forwarding of automated pre-recorded calls to customers for debt collection purposes was banned by the DPA.

The DPA provided several comments to IVASS [Italy's Insurance Companies Supervisor] in connection with preventing and countering fraud in third-party liability insurance policies for motor vehicles; the comments concerned, in particular, the claims database and the newly established registers of witnesses and injured parties, respectively. The DPA recommended that data subjects (including the individuals involved in a car accident, witnesses, etc.) should be informed appropriately; that the information identifying such data subjects should be retained for no longer than 5 years; that only the entities authorized by the law should be allowed to access the databases and exclusively in order to prevent and counter insurance fraud more effectively.

Based on sample checks, the DPA found several instances of unlawful processing of employees' and customers' data performed by department stores via video surveillance.

The DPA addressed the safeguards for data subjects in case customer care or telemarketing activities are committed to call centers located in third countries where no adequate data protection levels are in place compared to the EU. To that end, measures were laid down such as the obligation to provide thorough information and to notify the DPA beforehand of the call centers relied upon – via an ad-hoc form made available on the website – so as to enable the DPA to assess the scope of the transfers of personal data outside the EU.

Further to a prior checking application lodged by the Office of the Special Supervisor for the Archaeological Heritage of Naples and Pompeii, the DPA allowed a longer retention period for the video surveillance images collected in the building yards and the storage areas set up as part of *"Pompeii's Great Plan"* to support the prefecture in checking access to and attendance in the building yards with a view to preventing mafia-related activities.

A vademecum was drafted on "Joint Tenancy and Privacy" to address and provide guidance on the most frequent issues arising in this context.

NOVEMBER

A Memorandum of Understanding was signed with the Security Intelligence Department (SID) at the Prime Minister's Office to regulate information-gathering procedures related to the discharge of the DPA's and the Department's respective tasks. The MoU concerns, in particular, the information arrangements allowing the DPA to inquire into some key features of the data processing operations performed by intelligence and security bodies in specific areas – namely, cybersecurity or accessing the databases held by public administrative bodies or public utilities.

Instructions were issued to health care districts regarding the appropriate arrangements for the home delivery of medical appliances and devices so as to protect patients' privacy and dignity.

After a complaint was lodged with the DPA to have a parliamentary question de-indexed by search engines, as such question contained judicial data that had become obsolete due to supervening procedural developments, the competent bodies of the Italian Chamber of Deputies implemented ad-hoc internal procedural rules that were modeled after the interpretation and methodology developed by the DPA in similar contexts – i.e., in connection with de-indexing news stored in the online archives of major newspapers. Such rules were found to afford adequate protection in these specific situations as well.

In-depth prior checks were performed on the processing performed by the Revenue Agency for the purposes of the so-called "Redditometro" (Income-Meter). The DPA set forth various measures to be implemented in order to address the many criticalities found, which were related partly to the wording of the ministerial decree implementing the Income-Meter tool. The criticalities in question concerned quality and accuracy of the data used by the Agency; the estimated expenses incurred by each taxpayer as related to multifarious life-style components (recreational activities, purchase of books, dining-out habits, etc.), which envisaged allocation of the mean expense calculated by ISTAT [Italy's National Statistics Institute] to all the taxpayers in the Tax Register; and the information to be provided to taxpayers.

DECEMBER

The DPA launched a public consultation on the processing of personal data performed in connection with payments via smartphones and tablets as well as, generally speaking, via mobile remote payment services.

The DPA banned the processing of personal data relating to over 400,000 job applicants as performed by an employment brokerage website, because it was found to be in breach of both sector-specific legislation and data protection legislation.

SUMMARY OF KEY ACTIVITIES BY THE ITALIAN DPA IN 2013

A summary description of the activities carried out by the DPA in 2013 confirms what is by now one of the key features of the Garante, so much so that it can be said to have become part of its DNA: namely, the fact of dealing (or having to deal) with the most diverse issues and sectors where information flows impact the lives of individuals whether acting as citizens or consumers, employees, patients, and so on. There is an unrelenting tension between the social dimension of individuals, which fosters and sometimes requires the circulation of personal data (including sensitive data), and the need for fully respecting and protecting human dignity and fundamental freedoms. Proof of this is provided – if necessary – by the decisions and measures mentioned in the "Highlights" section, which are but a selection of the many issued in the past year - often as a result of inspections performed by the DPA.

1.1. *Technological developments, especially in electronic communications*, are still the focus of the DPA's attention in the light of the surveillance potential they harbor vis-à-vis the users of technology. This is unrelated to national borders, as pointed out in the letter the Garante sent to the Prime Minister to voice his concerns regarding the espionage practiced by the National Security Agency on the telephone and Internet communications also of Italian users. This, coupled with the evidence of the growing surveillance applied to a large portion of the population along with the retention of a wealth of personal information, led the Garante to firmly call upon the Italian Government to support, within the EU Council, the *adoption of the proposed reformation of the European data protection legislative framework* so as to strengthen its overall fabric. This objective was pursued unflinchingly by the DPA because of its importance, also in 2013, within the framework of the powers conferred on it. Following the so-called Datagate, the Garante was heard by the Parliamentary Commission for the Security of the Republic (Copasir) and on 11 November 2013 entered into a *Memorandum of Understanding with the Security Intelligence Department* (SID) at the Prime Minister's Office; the MoU is aimed at regulating information-gathering procedures related to the discharge of the DPA's and the Department's respective tasks. This concerns, in particular, the information arrangements allowing the DPA to inquire into some key features of the data processing operations performed by intelligence and security bodies in specific areas – namely, cybersecurity or accessing the databases held by public administrative bodies or public utilities.

To ensure that everybody can benefit the most from the wealth of information and the multifarious channels for participation made available by the Internet, the Garante decided to focus on *cyberbullying* for the European Privacy Day. The ultimate purpose was to make users, especially youths, aware of the dangers arising from the sometimes uninformed use (or misuse) of social networks whilst drawing the attention of institutional stakeholders – in particular, the Ministry of Education – to this highly sensitive issue.

The Net has obviously been the subject of decisions by the DPA as well. Spam, in particular, has long been the focus of attention by the DPA; however, it has developed of late into new forms such as *social spam* or *viral marketing* or *targeted spam*, which made it necessary to update the guidelines laid down by the DPA. A measure the Garante has long been enforcing to reconcile personal rights – in particular respect for personal dignity – with freedom of expression, i.e. the *de-indexation of news* stored in the online archives of major newspapers, continued to prove valuable and was actually implemented by the Chamber of Deputies via ad-hoc internal procedural rules; these were meant to afford adequate data protection in cases concerning parliamentary questions that contained "obsolete" information.

A public consultation was launched to better assess payment services via smartphones and tablets as well as – generally speaking – *mobile remote payment services*.

1.2. The DPA gave a favourable opinion on a draft legislative decree concerning *transparency obligations of public administrative bodies*, which was adopted on 14 March 2013. A key area

where such transparency is ensured is exactly the Web, thanks to institutional websites, and this is why the Garante highlighted some criticalities in this regard by taking account also of the EU regulatory framework and the stance taken by the Court of Justice of the EU. The guidance provided by the Garante was followed only partly, whilst it was aimed ultimately at making sure that transparency would not be in conflict with the right to privacy and the protection of personal data – e.g. by refraining from disseminating medical information or data on disadvantaged situations applying to the beneficiaries of welfare allowances. A source of concern is the *publication on the Internet of sensitive data by municipalities* via their respective notice boards online – this is the case, for instance, of the posting of municipal orders for obligatory medical treatment; in yet other cases the dissemination of excessive data relating to single individuals or employees was stigmatized by the Garante via prohibitory injunctions.

1.3. The motley features of the Net are only one of the areas tackled by the DPA, and it must be said that enforcing the law in this sector is made all the more difficult by the geographic constraints placed on the scope of application of personal data protection legislation – which constraints are expected to be overcome thanks to the *draft data protection Regulation*. The latter would also apply to the processing of personal data relating to individuals residing in the EU in connection with products or services offered to them, or in order to monitor their behavior, regardless of whether such processing is performed by controllers established in third countries. Indeed, the Garante's focus continues to be on other processing operations that may considerably affect individuals' rights – as shown actually by the significant increase in administrative procedures for the imposition of sanctions; this applies, first and foremost, to the *processing of sensitive and judicial data*, and the Garante renewed, on 12 December 2013, the general authorizations to process such data which were then published in Italy's Official Journal (No. 302 of 27 December 2013). In this connection, it should be recalled that the DPA received – as usual – a considerable number of complaints relating to the allegedly *inappropriate processing of health-related data* both in health care and in other contexts. This led the Garante to require that suitable arrangements be made, also of a technical nature, to ensure that the information contained in health care records would only be accessible to the practitioner and/or the facility where such records were created and could only be shared with other practitioners treating a data subject at other medical units or wards with the data subject's specific consent – which may also apply to medical information relating to past clinical events. In a broader perspective, the DPA kept on supervising the issues related to the nationwide deployment of the *Electronic Health Care Record*.

The DPA required health care districts that had installed *video surveillance* equipment in the restrooms of the respective facilities for ruling out drug addiction cases to take measures and precautions such as to protect the privacy of any individual whose urine sample was being taken – in particular, the DPA banned the recording of CCTV images by whatever means. Similarly, measures and arrangements were laid down to ensure that health care districts would implement appropriate mechanisms with a view to the *home delivery of medical devices* and equipment so as to protect patients' privacy and dignity. The same rationale underlies a decision adopted by the DPA – which informed Regions, Autonomous Provinces and INPS [the national social security agency] accordingly – whereby the competent medical boards must not include the patient's clinical history, medical findings and diagnosis in the *invalidity certification* that is to be submitted under the law in order to obtain, for instance, the car pass for restricted access areas or the tax deductions granted when purchasing motor vehicles.

The DPA's activities in respect of the processing of health-related data do not limit themselves to issuing orders and injunctions and performing inspections, since the DPA has long been cooperating substantially with the relevant stakeholders. The DPA participates in several working groups and has issued several opinions to ensure that data subjects' privacy and dignity would be respected in implementing data processing rules. Reference should be made in this regard to the opinion rendered on the draft agreement between Government, Regions and the Trento and

Bozen Autonomous Provinces concerning the *guidelines for the assessment of the use of human cells and tissues* (corneas, skin, heart valves) for experimental transplantations and new advanced drug therapies: the DPA requested that aggregate data be used to prevent the patients concerned from being identified, also indirectly.

1.4. As for *large databases*, the DPA kept the focus of its attention also on *data retention* issues – which were recently the subject of an important judgment by the EU Court of Justice (joined cases C-293/12 and C-594/12) published on 8 April 2014 regarding the relevant EU legislation. Thanks to the collaboration with the Financial Police, the DPA performed sample inspections to verify compliance with the measures it had laid down ever since 2008 on Internet and telephone traffic data retention; the sanctions envisaged in the Code in case of non-compliance with previous orders by the DPA were also imposed.
Still regarding the electronic communications sector, a decision was adopted in pursuance of the legislation on *personal data breach notification* to provide guidance on who was required to fulfil the relevant obligations (under Sections 32 and 32-a of the Code), what measures could ensure minimum common security standards, the timeline and contents of the notification – which may also be given via an ad-hoc downloadable form on the DPA's website.

1.5. *Video surveillance* remains one of the key areas of the DPA's activity, both in the public and in the private sector. Some specific cases deserve being mentioned here: in one case, the DPA banned the use of webcams in a *nursery school* to protect children's privacy and the unfettered development of their personality as well as to ensure that their relationships with teachers would be free from whatever constraints and to safeguard freedom of teaching. Conversely, the DPA gave the green light – subject to the adoption of suitable safeguards as set out by the Garante following a prior checking application – to the deployment of a "smart" video surveillance system in a municipality in order to counter *vandalism*; on-screen real-time alerts are displayed on monitoring workstations whenever a person remains for long in areas close to certain monuments and institutional bodies.
Balancing security and fundamental rights was an exercise the DPA carried out also in other areas. For instance, the DPA banned police headquarters to process the images collected via *CCTV cameras installed in streets* for public safety purposes as such cameras also allowed viewing inside people's homes. Following a prior checking application lodged by the Office of the Special Supervisor for the Archaeological Heritage of Naples and Pompeii, the DPA allowed a longer retention period for the video surveillance images collected in the building yards and the storage areas set up as part of "*Pompeii's Great Plan"* to support the prefecture in checking access to and attendance in the building yards with a view to *preventing mafia-related activities*.
Reference can also be made to the physical and IT measures and arrangements laid down by the Garante in an important decision that was aimed at enhancing security of the personal data collected and used as part of *interception activities* by the CITs (Telecommunications Interception Centres) attached to each Prosecuting Office as well as to police offices tasked with performing interceptions for judicial authorities.

1.6. As part of a *simplification* plan that was launched long ago, the DPA drafted a guidebook (Vademecum) on "*Joint Tenancy and Privacy*" plus an additional one called "*Privacy: Working with Business* – Ten Corporate Best Practices to Improve Your Business". They provide practical advice in a concise manner to ensure compliance with data protection laws and foster implementation of the relevant measures.
The DPA brought some clarification and introduced *simplified arrangements also in connection with marketing activities*, an issue that is especially sensitive. In particular, it was clarified that a data controller obtaining data subjects' consent for direct marketing purposes via automated mechanisms may process the relevant data also according to conventional mechanisms (correspondence, operator-assisted phone calls) unless the data subjects object to the

processing. At the same time, the DPA implemented *additional measures to counter "wild" telemarketing and unsolicited marketing*, as several inspections were carried out and injunctions were issued against two major IT companies specializing in database services, which had to pay hefty fines as they had failed to comply with orders the DPA had already issued in their regard.
Safeguards for data subjects were also laid down in case customer care or telemarketing activities are committed to *call centers located in third countries* where no adequate data protection levels are in place compared to the EU. To that end, measures were laid down such as the obligation to provide thorough information and to notify the DPA beforehand of the call centers relied upon – via an ad-hoc form made available on the website – so as to enable the DPA to assess the scope of the transfers of personal data outside the EU.

1.7. Another sector where the DPA stepped in has to do with the appropriate *use of personal information to counter fraud*, which must take place on the basis of clear-cut legal rules. Several remarks were made accordingly to IVASS, i.e. the Insurance Companies' Supervisor, in connection with preventing and countering *fraud in third-party liability insurance policies for motor vehicles*; the comments concerned, in particular, the claims database and the newly established registers of witnesses and injured parties, respectively. The DPA recommended that data subjects (including the individuals involved in a car accident, witnesses, etc.) should be informed appropriately; that the information identifying such data subjects should be retained for no longer than 5 years; that only the entities authorized by the law should be allowed to access the databases and exclusively in order to prevent and counter insurance fraud more effectively. Regarding *consumer credit fraud* and, in particular, *identity thefts*, criticalities were pointed out in a draft decree by the Ministry of Economy and Finance that was meant to regulate operation of the public system for the administrative prevention of this type of fraud. As well as requesting compliance with purpose limitation requirements and the adoption of adequate security measures, the DPA found it necessary to include, in the relevant regulations, specifications on the different access arrangements applying to "direct" and "indirect" participants; furthermore, the DPA suggested including measures to inform data subjects of any data inconsistencies as found in the public databases following the checks to be performed.
Another issue the DPA addressed – as it had already done also via an *omnibus* decision – has to do with *debt collection*; in particular, the DPA banned the forwarding to customers of pre-recorded, operator-unassisted phone calls for debt collection purposes.

1.8. Personal information is used increasingly to counter *tax evasion*, which remains a major issue in Italy in spite of the many measures – including legislative ones – implemented over the past few years. The DPA's focus in this regard was on ensuring that fundamental rights of individuals would not be violated unjustifiably. This is why in-depth prior checks were performed on the processing performed by the Revenue Agency for the purposes of the so-called "Redditometro" (*Income-Meter*), whereupon the DPA set forth various measures to be implemented in order to address the many criticalities found, which were related partly to the wording of the ministerial decree implementing the Income-Meter tool. The criticalities in question concerned quality and accuracy of the data used by the Agency; the estimated expenses incurred by each taxpayer as related to multifarious life-style components (recreational activities, purchase of books, dining-out habits, etc.), which envisaged allocation of the mean expense calculated by ISTAT [Italy's National Statistics Institute] to all the taxpayers in the Tax Register; and the information to be provided to taxpayers.

1.9. *Biometrics* have been the subject of in-depth studies and measures by the DPA both in connection with prior checking applications and following on-the-spot inspections. The DPA allowed two banks to equip their financial promoters with tablets that could perform the *graphometric analysis* of the signature affixed by any customer entering into financial agreements in electronic format; at the same time, the companies involved in enabling and

managing both systems were required to take special measures to protect the data they collected along with measures to afford bank customers the option to undersign such agreements via conventional mechanisms as well.

1.10. Conversely, the DPA found that the use of *biometrics to check attendance of teachers and administrative staff* in some schools was disproportionate – in line with the stance taken long ago by the DPA in this regard. It is actually in *the occupational context* that the substantial number of complaints received by the DPA – which were often found to be substantiated following inspections – points to persistent breaches of personal data protection legislation and sector-specific laws. This applies, in particular, to the legislation on remote surveillance of employees, in spite of the simplified procedural measures that were introduced by the Ministry of Labour and Welfare via a circular letter of 16 April 2012 concerning installation of audio-visual devices. The criticalities are especially remarkable in connection with *video surveillance of employees* - based on sample checks concerning department stores, the DPA found that in some cases the security company tasked with managing the system to prevent robberies and shoplifting had not been granted the necessary authorization by the governmental *prefect*; however, the *complaints* also related to surveillance tools that can be detected less easily by data subjects – such as geolocation equipment or software to monitor online navigation as performed via the electronic communications devices provided to employees. These issues have long been the subject of ad-hoc decisions by the DPA.

The severe occupational crisis that is gripping our country has resulted into a substantial increase in the number of job applicants, who rely on the most diverse brokerage systems. The latter include entities that manage Internet websites (as actually envisaged by the law subject to compliance with specific requirements) and thus process huge amounts of personal data. Against this background, which deserves more in-depth analysis, it should be recalled here that the DPA banned the processing of personal data relating to over 400,000 job applicants as performed by an *employment brokerage website*, because it was found to be in breach of both sector-specific legislation and data protection legislation.