

Annual Report 2016 – Summary of the Activities by the Italian DPA

The Annual Report on the Italian Data Protection Authority's 20th year of activity was submitted to Parliament on the 6th of June, 2016. The DPA's Panel of Commissioners includes Antonello Soro, Augusta Iannini, Giovanna Bianchi Clerici, and Licia Califano.

As well as taking stock of the activities performed in 2016, the Report outlines the future scope of action of the DPA in order to ensure the effective protection of personal data – especially online –, partly in the light of the forthcoming application of the new EU General Data Protection Regulation (May 2018), as well as to meet the challenges arising from the new economic growth models and the increasing demand for protection coming from individuals.

Key Areas of Activity

The main areas addressed by the Italian DPA in 2016 included cybercrime and cybersecurity; online profiling and social media; Internet-related risks and cyberbullying; the fight against terrorism and mass surveillance; Big data; the use of new technology in the workplace; the online transparency of public administrative bodies and the safeguards for citizens; taxation regimes and the protection of taxpayers' privacy; telemarketing; interceptions and protecting data contained in judicial case files; protection of children by the media; consumer rights; large public databases; education and schools; the right to be forgotten; safeguards for data transfers to the USA; and health care.

The DPA continued its work aimed at ensuring the protection of privacy in the online world, starting from search engines and social networks. In 2016 **Google** complied with the undertakings contained in the verification protocol it had submitted to the DPA with a view to bringing the processing of users' data into line with the Italian legislation. The DPA ordered **Facebook** to stop fake accounts and improve transparency and user control.

Regarding the Internet, the DPA participated in an international survey on IoT-related issues and focused, in particular, on domotics. Further, it banned the implementation of a project whereby reputational analysis would be committed exclusively to an algorithm.

The DPA worked throughout 2016 to clarify the major innovations brought about by the new EU General Data Protection Regulation (**GDPR**); along with the other EU DPAs, it contributed to drafting guidelines (on DPOs, data portability, the role of lead authorities, and data protection impact assessments) with a view to the GDPR full application in our country.

The criteria for reconciling **right to be forgotten** requests with collective memory were clarified; the right to have online archives of newspapers updated was strengthened further.

Regarding **cybersecurity**, the DPA carried on its oversight activities in 2016 and took steps both of its own motion and following specific reports or complaints concerning data breaches. Data breach notifications by public bodies totalled 15.

As for the private sector, a trend observed in the previous year continued in 2016 as well – namely, **43** data breaches were notified by some of the main providers of publicly available electronic communications services as established in our country.

In the **health care** sector, the DPA stepped in to regulate the use of fingerprints to enable access to hospitals. It also provided guidance on the public cancer registry, the new transplantation information system, and assisted reproduction techniques.

As for schools, the DPA published guidelines to help students, families, teachers and educational organizations to navigate the data protection world with ease. It gave its green light to access by universities to the national students' registry.

Regarding workplace issues, the DPA set forth rules on using new technologies following enactment of the so-called 'Jobs Act'.

The DPA called upon the government to reconcile **online public administrative transparency** with citizens' privacy and dignity; it also banned the online dissemination of sensitive data in a few cases.

Specific steps were taken to enhance IT systems security in the public sector and increase safeguards for citizens in the SPID (digital identification public system) implementing phase.

Regarding tax matters, in particular the new **pre-filled tax return ('730') form**, the DPA stepped in to enhance security measures in connection with access by intermediaries as well as to lay down data retention periods.

The DPA's special commitment continued in 2016 to bring major public databases into line with security requirements – foremost among them being the **Taxpayers' Registry**.

The Business Information Code of Conduct came into force in 2016; the CoC had been adopted by the DPA to reconcile business requirements with fairness principles in processing reliability data related to entrepreneurs and corporate managers.

A 'vademecum' was published to highlight the appropriate procedures in debt collection.

Several measures were taken regarding the increasingly widespread use of biometrics and profiling in many business sectors.

Work continued to prevent **unregulated ('wild') telemarketing** – which is unfortunately on the rise. The DPA found major breaches by telephone companies; carried out inspections at some Albanian call centres and put forward proposals for Parliament to enhance the safeguards afforded to citizens.

The **privacy/journalism** (right to inform) relation was another key area in particular as for the protection of children.

A Few Figures

561 decisions were adopted by the panel of the DPA's Commissioners in 2016.

About **4,600** inquiries, claims and reports were handled with particular regard to telemarketing, consumer credit, video surveillance, private bodies outsourced by public administrative entities, debt collection,

credit and banking, insurance companies, Internet, journalism, health care and welfare services, local authorities.

277 complaints were adjudicated mainly concerning publishing houses (including TV companies), banks and financial companies, public and private employers, credit bureaux, public administrative bodies and public service outsourcing.

20 opinions were rendered to Government and Parliament ranging from police and intelligence services to the computerisation of public administrative databases and judicial proceedings, taxation issues, SPID, the electronic students' and teachers' card, and health data.

9 hearings by Parliament were held concerning first and foremost telemarketing rules, the fight against terrorism, transparency rules and video surveillance.

The DPA lodged reports with judicial authorities in **53** cases – in particular due to the failed adoption of minimum security measures.

The number of **administrative violations** found in 2016 was on the rise (by 38%) compared to 2015, totalling **2,339**. A substantial portion among them (1,817) consisted in the failure by electronic communications service providers to notify data breaches (to data subjects and/or the DPA), followed by cases where data were processed unlawfully – mainly because of the lack of consent – or by providing no or flawed information to users on the processing of their personal data; the excessive retention of telephone and Internet traffic data, the failure to take security measures, and the non-disclosure of documents as requested by the DPA along with the failure to comply with measures adopted by the DPA were also found.

The **administrative fines** levied totalled about **3.3 million Euro**.

282 on-the-spot inspections were carried out, partly with the help of the Privacy Squad at Italy's Financial Police. The targeted entities belonged to several areas in both the public and the private sectors. As for the latter, the inspections concerned mostly car sharing companies, web marketing and telemarketing companies along with gene research businesses, job placement agencies, IT technical support and data retrieval companies, online gaming businesses and financial companies. A major inspection was carried out regarding money transfer companies as part of anti-money laundering activities, leading to the imposition of fines totalling 11 million Euro. As for the public sector, the inspections focused on agencies providing tax-related consultancy and support, major public databases and taxation bodies with particular regard to security measures and internal audits.

As for public outreach, over **24,000** requests for information were handled concerning, in particular, unsolicited marketing calls (33%), the requirements arising from the new GDPR (11%), Internet, video surveillance, unsolicited mails, faxes and text messages, data protection in the workplace and banking transactions.

International Activities

No less important and demanding was the work carried out by the DPA at international level. Considerable importance was attained by the work related to the reform of the EU data protection framework, i.e. the so-called 'data protection package'; the package was finalised by the adoption of the new General Regulation (which came into force on 24 May 2016) and the Directive on the processing of personal data

for judicial and police purposes (which came into force on 5 May 2016). The Garante followed the discussion on the revised EU legal framework throughout, in particular by participating as a technical expert in the meetings of the competent DAPIX working party at the EU Council.

A major area of activity was related, as usual, to the work by the 'Article 29 Working Party' of the EU DPAs where President Soro acted as Vice-Chair throughout 2016. As well as working on important guidance with a view to implementing the new GDPR, the DPA actively contributed to drafting several opinions and documents adopted by the Working Party which addressed, among other things, the future e-privacy regulation (in the electronic communications sector), social media (Facebook and WhatsApp, in particular), big data, data protection in the financial sector, data published for transparency purposes in the public sector, data transfers abroad with regard to binding corporate rules and standard contractual clauses along with judicial and police cooperation issues.

Especially significant was the adoption of an opinion with a view to the new EU-USA data transfer agreement, i.e. the so-called Privacy Shield.

The DPA also contributed to the work in progress at the Council of Europe in order to revise the 1981 data protection Convention as well as to draft Big Data guidelines; OECD initiatives were also followed carefully with particular regard to security and privacy in the digital economy. Cooperation with international groups fostering targeted joint enforcement initiatives such as the Global Privacy Enforcement Network (GPEN) was strengthened as well.

Finally, reference should be made to the in-depth activities carried out by the DPA as a member of the Schengen, Europol, Eurodac, CIS (Customs Information System) and VIS (Visa Information System) joint supervisory authorities.

Cooperation agreements were entered into with similar authorities in Eastern European countries to foster information exchanges and joint initiatives including inspections.

Rome, 6 June 2017