SUMMARY

back

- **Data Protection Code - Legislative Decree no. 196/2003**

Introduction

Italy's consolidated data protection code came into force on 1 January 2004.The Code brings together all the various laws, codes and regulations relating to data protection since 1996.

In particular, it supersedes the Data Protection Act 1996 (no. 675/1996), which had come into effect in May 1997.

There are three key guiding principles behind the code, which are outlined in section 2:

1. Simplification
2. Harmonisation
3. Effectiveness

The code is divided into three parts.

The first part sets out the general data protection principles that apply to all organisations.

Part two of the code provides additional measures that will need to be undertaken by organisations in certain areas, for example, healthcare, telecommunications, banking and finance, or human resources.

Part three relates to sanctions and remedies. It is expected that the second part of the code will be developed further through the introduction of sectoral codes of practice.

Scope of the Italian data protection code - The code applies to all processing within the State and its territories. It will also affect outside organisations that make use of equipment located within Italy, which could include e.g. PCs and other computer-based systems (see Section 5 of the Code). If an organisation outside the EU is processing data on Italian territory, it must appoint a representative in Italy for the application of Italian rules (this will be necessary for notifying with the Garante, if notification is due, and providing data subjects with information notices).

Main Features of the Data Protection Code

Notification - One of the key targets for simplification was the notification process, which was made more straightforward compared to the 1996 Act in line with the EU Data Protection Directive - which allows the notification process to be simplified in cases where data processing does not adversely affect the rights and freedoms of data subjects (see Article 18(2) of the directive). Under the Italian code, organisations are only required to notify the Garante when processing higher-risk categories of data. These include, in particular, genetic and biometric data, data processed for the purpose of analysing or profiling individuals, and credit-related information (see Section 37 of the code for additional details). This approach is also aimed at making the process more transparent and understandable for individuals.

Data minimisation - Section 3 of the code introduces the element of data minimisation into Italian data protection. The code encourages organisations to make use of non-personal data whenever possible.

Data subjects' rights/Decision taking - The code aims to strengthen individuals' data protection rights, allowing them to exercise their rights and instigate proceedings more easily. In an effort to simplify the complaints process, the Garante has published a complaints form on its website. The Garante can also order businesses to abide by compliance requirements set out in its decisions. When responding to investigations, businesses now have 15 days to comply, compared to the previous 5-day timeframe. The turnaround for dealing with complaints has been raised to 60 days (previously it was 30 days); this period was found to be suitable in order for the Garante to work effectively and the parties to prepare their pleadings appropriately.

International Data Transfers - The data protection Code has incorporated and, to some extent, updated the previous rules on data transfers (data transfers are addressed in Sections 42-45 of the Code). Whereas previously businesses had to notify the Garante of their intention to transfer data outside the EU, under the new system companies will only have to provide notification in cases in which the transfer of data could prejudice data subjects' rights (see the Notification section). Additionally, the new system does not require organisations to resubmit notifications each year The rules for legitimising transfers to non-EU countries can be found in Section 43 of the Code and include consent, meeting contractual obligations, public interest requirements, safeguarding life/health, investigations by defence counsel, use of publicly available data, processing for statistical/historical purposes. Additional provisions for legitimising transfers are laid out in Section 44 of the Code and include transfers to countries deemed adequate by the European Commission, the adoption of contractual safeguards, and the use of binding corporate rules. Data subjects are entitled to lodge claims in Italy for non-compliance with the said contractual/corporate safeguards.

Main Features in Respect of Specific Processing Operations

Human Resources Data - The code has fully implemented Article 8 (b) of the EU directive which applies to the processing of data. Organisations processing sensitive data that wish to find an alternative to the somewhat unreliable issues of employee consent, can look at the exemptions laid out in Section 26 of the code. For example, Section 26 (4d) allows the processing of sensitive data without consent if necessary to meet obligations under employment law.

Health data - Processing is allowed with the data subject's consent (which must be provided in writing) and the Garante's authorisation if the data controller is a private body. As for public bodies, processing is allowed if it is provided for in laws/regulations; however, the latter must set out the specific processing operations and purposes in detail, otherwise the relevant public bodies must specify them via ad-hoc regulatory instruments. The data subject's consent is not required, in principle, whilst the Garante's authorisation is necessary except for the processing by health care professionals that is indispensable with a view to the data subject's health and/or bodily integrity. The Garante's authorisation has been granted in the form of an instrument applying to several entities and/or processing operations, i.e. as a "General Authorisation for the Processing of Sensitive Data" by various categories of data controller (see Legislation section). It should be recalled that specific provisions are laid down in the DP Code to regulate the processing of medical data in the health care sector (Sections 75-94). In particular, health care professionals and public health care bodies may process medical data (the Code refers to "data suitable for disclosing health") with the data subject's consent and without the Garante's authorisation if the processing concerns data and operations that are indispensable with a view to the data subject's health and/or bodily integrity; conversely, they may process medical data without the data subject's consent but with the Garante's authorisation if the processing is indispensable to safeguard public health.

Electronic Communications Data - The Code has implemented the provisions contained in the E-Communications privacy directive 2002/58/EC as well as in the data retention directive (2006/24/EC) (see Title 10, Part 2 of the Code). One of the main principles is on electronic marketing which requires organisations to obtain prior consent before sending electronic marketing to consumers (see Section 130). This applies to all forms of e-marketing, including e-mail, fax, SMS/MMS etc.. Specific provisions were added to regulate telemarketing. There is also a ban on sending e-marketing from anonymous addresses - this is a breach of the data protection code as the data controller has withheld its identity. As for data retention, communications service providers (CSPs) are permitted to retain traffic data for only a six-month period in order to deal with disputes over billing and subscriber services (section 123(2)). CSPs are also required to retain traffic data for longer in connection with law enforcement purposes; the retention periods are currently set at twenty-four months (telephone traffic data) and twelve months (electronic communications traffic data), irrespective of the given offence at issue (in pursuance of directive 2006/24/EC) (see section 132). Following ratification of Council of Europe's Cybercrime Convention (via Act no. 48/2008, which amended Section 132 of the DP Code), police authorities were enabled, under specific circumstances, to order IT and/or Internet service providers and operators to retain and protect Internet traffic data - except for contents data- for no longer than ninety days, in order to carry out pre-trial

investigations or else with a view to the detection and suppression of specific offences. The order issued by police authorities must be notified to and validated by the competent public prosecutor.

Main Features as to Compliance and Enforcement

Complaints - Data subjects can settle disputes either through the courts or by lodging a complaint with the Garante in case they have been prevented from exercising access/erasure/rectification/updating rights (as per Section 7 of the code).Organisations have 30 15 days to respond and can appeal to the Garante for more time. The Garante will then have 60 days to consider the request (see above "Data Subjects' Rights/Decision Taking").

Inspections - The Garante's inspection powers are laid out in Section 158 of the code. When investigating organisations, the Garante can request information and documents, although these requests are not legally binding. However, if there is no cooperation, and the organisations refuses access to its systems, the Garante can apply for a judicial order to carry out an investigation.

When carrying out formal inspections, the Garante can demand copies of manual records and databases, which may be passed onto the judicial authorities. A report of the outcome is then published.

back

Codes of Conduct

Introduction

Legislative decree 196/2003 has enhanced the importance of codes of conduct and professional practice in respect of the protection of personal data.

In particular, it provides for their adoption in several, highly significant sectors such as processing of data via the Internet and/or in the employment context, for purposes of direct marketing, by private credit reference agencies, or in connection with video surveillance activities. The main principle in this connection is that compliance with the provisions set forth in the relevant code of conduct is a prerequisite for the processing operations to be lawful - see section 12(3). Adoption of the codes of conduct takes place following the impulse given by the Italian DPA with the involvement of the relevant industry sector; a specific procedure is envisaged and the final instrument is to be published in Italy's Official Journal (the official collection of legal and regulatory instruments). This section contains the codes adopted so far in the various sectors and will be updated as appropriate.

- Code of Practice Applying to the Processing of Personal Data Performed with a View to Defence Investigations

- Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments

- Code of conduct and professional practice applying to processing of personal data for statistical and scientific purposes

- Code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the national statistical system

- Code of conduct and professional practice Regarding the processing of personal data For historical purposes

- Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities

- Code of Ethics and Conduct in Processing Personal Data for Business Information Purposes

back

General Authorisations Issued for the Processing of Sensitive Data (as currently in force)

Introduction

An authorisation by the Italian DPA is required to enable private bodies to process sensitive data (see Section 26 of the DP Code). Additional safeguards apply to the processing of judicial data. To prevent private-sector data controllers from having to apply for ad-hoc authorisations, the DP Code provides (Section 40) that "general authorisations" may also be issued by the Italian DPA. Such general authorisations may be targeted to industry sectors (e.g. banking and insurance companies) and/or specific categories of data (e.g. genetic data or medical data).Where a data controller complies in full with the provisions made in the relevant general authorisation, no ad-hoc authorisation will be required. If this were not the case, a specific application will have to be lodged with the Italian DPA; the DPA will then consider all the circumstances of the case and decide whether the authorisation is to be granted. The general authorisations currently in force for the processing of sensitive data expire on 31 december 2013.

- Authorisation No. 1/2014 Concerning Processing of Sensitive Data in the Employment Context

- Authorisation No. 2/2014 Concerning Processing of Data Suitable for Disclosing Health or Sex Life

- Authorisation No. 3/2014 Concerning - Processing of Sensitive Data by Associations and Foundations

- Authorisation No. 4/2014 Concerning - Processing of Sensitive Data by Self-Employed Professionals

- Authorisation No. 5/2014 Concerning - Processing of Sensitive Data by Various Categories of Data Controller

- Authorisation No. 6/2014 Concerning Processing of Sensitive Data by Private Detectives

- Authorisation No. 7/2014 Concerning Processing of Judicial Data by Private Entities, Profit-Seeking Public Bodies and Public Entities

- Authorisation No. 8/2014 for the Processing of Genetic Data

- Authorisation no. 9/2014 - General Authorisation to Process Personal Data for Scientific Research Purposes

back

General Authorisations Issued for Cross-Border Data Flows to Third Countries

Introduction

This section includes the authorisations issued by the Italian DPA to enable data controllers (both public and private) to transfer personal data to third countries that have been found by the European Commission to provide "adequate" data protection safeguards. The adequacy decisions made by the European Commission are among the preconditions to transfer data to non-EEA countries (see Article 25(6) of

directive 95/46/EC). This provision has been transposed into Section 44(1)b. of the DP Code. Additionally, to prevent data controllers from having to apply for ad-hoc authorisations, the DP Code provides (Section 40) that "general authorisations" may also be issued by the Italian DPA. Where a data controller complies in full with the provisions made in the relevant general authorisation, no ad-hoc authorisation will be required for the data transfer. The Italian DPA reserves the right to investigate the processing arrangements and, where appropriate, block or ban the data transfer.

- Authorisation to Transfer Personal Data from the Italian Territory to the Eastern Republic of Uruguay

- Authorisation to Transfer Personal Data from the Italian Territory to New Zealand

- Authorisation to Transfer Personal Data from the Italian Territory to the State of Israel

- Authorisation to Transfer Personal Data to the Principality of Andorra

- Authorisation for data transfers to the US based on the "Safe Harbor Principles" (**PRESS RELEASE: Data Transfers to the USA: the "Safe Harbor" Authorisation is Invalid** - 6 november 2015)

- Authorisation for data transfers to Switzerland

- Authorisation for data transfers to Hungary [no longer in force]

- Authorisation for data transfers in compliance with Standard Contractual Clauses (controller-to-controller) (First Set)

- Authorisation for data transfers in compliance with Standard Contractual Clauses (controller-to-processor)

- Authorisation for data transfers to the Bailiwick of Guernsey

- Authorisation for data transfers to Canada

- Authorisation to Transfer Personal Data from the State's Territory to Third Countries

- Authorisation for data transfers to the Isle of Man

- Authorisation for the Transfer of Personal Data from the State's Territory to the US CBP Office of the Department of Homeland Security

- Authorisation for data transfers to Argentina

back

Other Items of Legislation

- Presidential Decree no. 178 dated 7 September 2010 - Regulations on setting up and management of the public register of subscribers opting out of the use of their phone numbers for the purposes of commercial selling and/or promotions

- Legislative decree no. 109 dated 30 May 2008 - Transposition of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communication Services or Public Communications Networks and Amending Directive 2002/58/EC

- Legislative decree no. 144 dated 2 August 2007 - Implementing Directive 2004/82/EC on the Obligation of Carriers to Communicate Passenger Data