diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 10/03/2016

All'indirizzo http://www.diritto.it/docs/37916-data-breach-notification-obligations-summary-overview-of-the-current-eu-italy-legal-framework-in-light-of-the-european-general-data-protection-regulation-and-network-information-security-directiv

Autori: Marcoccio Gloria , Corsini Ettore

Data Breach notification obligations: summary overview of the current EU/Italy legal framework in light of the European General Data Protection Regulation and Network Information Security Directive

Data Breach notification obligations: summary overview of the current EU/Italy legal framework in light of the European General Data Protection Regulation and Network Information Security Directive

Gloria Marcoccio - gloria.marcoccio@glory.it, Ettore Corsini - corsiniettore@gmail.com

Introduction

The information and networked society services are inextricably linked to our professional activities as well as social & private life, and processing of data (not only personal data) is the thread and essential basis for the actual operation of such services.

As such, data has become one of the most regulated assets, also with specific attention to the required security measures and obligations to notify incidents toward the relevant competent authorities and, in some cases, toward the affected subjects.

In this scenario, the last year has brought significant news at EU legislation level in particular with the agreed texts of the European Data Protection Regulation (GDPR) which will replace the present UE Privacy directive 95/46/EC, and the European Directive on Network and Information Security (NIS) which will bring specific requirements about security in the sectors of Essential Services and Digital Services (for the meaning of such terms please refer to the following figure).

Among the other requirements, such EU new legislations set out obligations about data breach/incident notification where for some specific cases the regulations already exist both at EU and Member States level.

This article provides an overview on data breach/incident laws, focus on EU and Italy contexts, and proposes some food for thought to the companies addressees of such rules, especially when possible overlapping of requirements involves attention and coordination in order to fulfill the relevant laws, avoiding costly and duplicated actions.

Overview of the already existing EU-Italy laws about data breach / incidents notification

At EU level the first regulation about personal data breach already in force is in the sector of publicly available electronic communication services, article 4 of the so called E-privacy directive 2002/58/EC as amended by Directive 2009/139/EC. This directive specifies that personal data breach means "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community*". The 28 Member States have made the transposition of article 4 E-privacy directive into their national legal frameworks: in Italy such transposition is represented by article 32-bis of the Italian Legislative Decree 196/03 (Privacy Code). Furthermore in Italy the Italian Data Protection Authority (DPA) issued a specific Measure in April 2013 with additional detailed requirements. Afterwards and with the aim to achieve a suitable level of harmonization with regard to the personal data breach notification rules in all the Member States in the electronic communication sector, the European Commission enacted the specific Regulation 611/2013: since it is an European Regulation, it is directly applicable in all the Member States without any need of national transposition measures and it overrides on possible national conflicting laws.

Then in the year 2014, in the sector of Trust services (they deal with the creation, verification, validation and preservation of electronic signatures, seals, time stamps and certificates for website authentication), the European Regulation 910/2014 with its article 19 has set out data breach notification obligations for " *any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein*".

In Italy in November 2014 the Italian DPA has issued a Measure for the processing of biometric data in which notification obligations exist in case of " *any data breaches and/or any IT incidents (such as unauthorized access or malware actions) that may expose such data to the risk of a breach even though they do not impact biometric data directly*".

In June 2015 the Italian DPA has issued a Measure about the processing of health data in the context of the Health Data Dossier (processing performed by health bodies, both in the public and private sectors such as hospitals, health care centers,...) which includes breach notification obligations regarding any data breaches and/or any IT incidents (such as unauthorized access or malware actions) that may expose at risk the data contained in the Health Data Dossier; then in September 2015 it has been enacted the Italian decree 178 of the President of the Council of

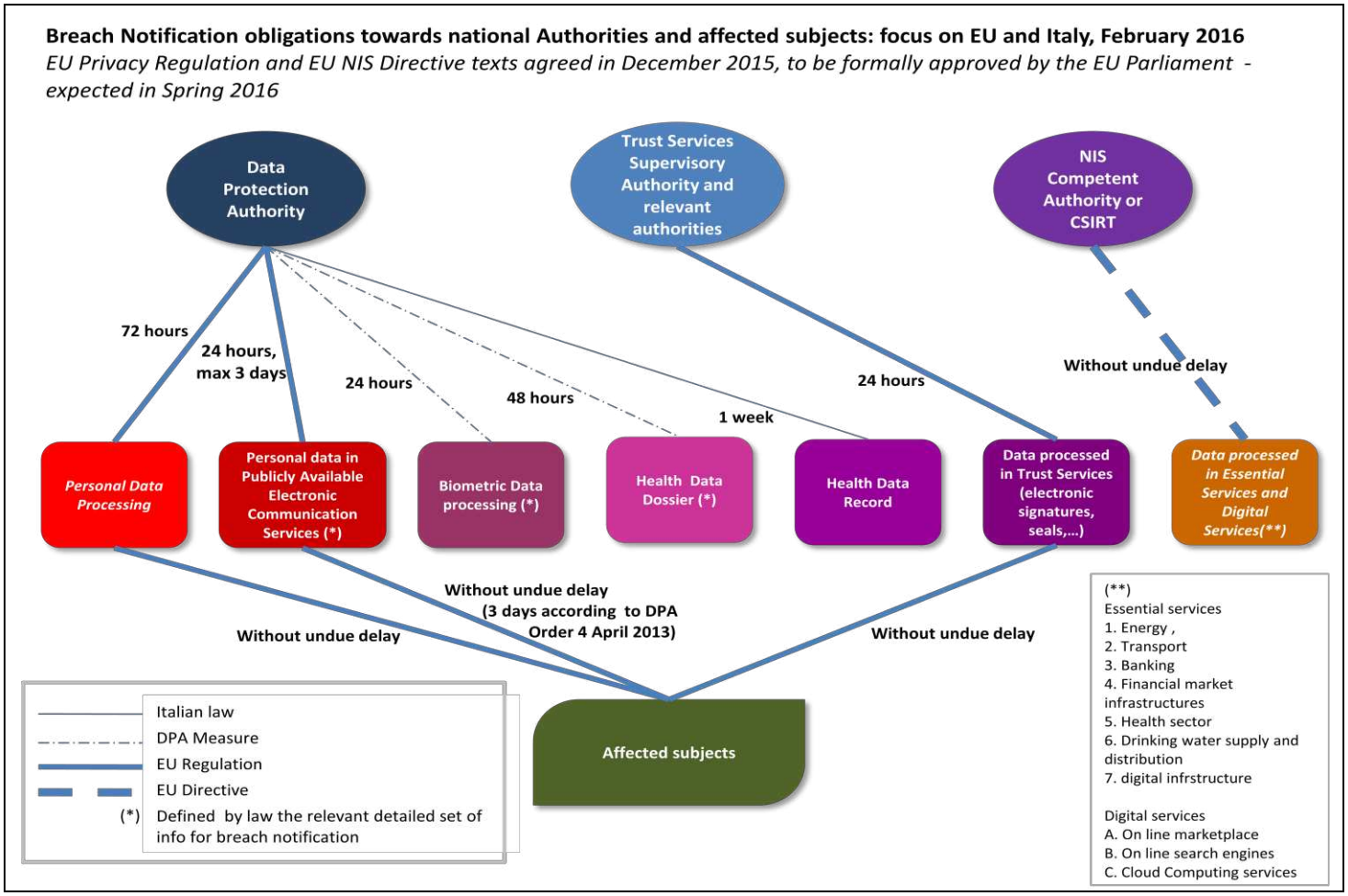
Ministers (DPCM) which, with its article 23 about security and data retention requirements, includes breach notification obligations in case of any data breach involving loss, destruction or undue dissemination of data contained in the Health Data Record[1].

Summary overview about the overall legislation context for data breach notification obligations

Breach notification obligations as a rule provide for the fulfilling of specific timing and content requirements

- always: notification toward the national competent authorities,
- when specific risks arise: in addition notification toward the affected subjects. According to each specific service context identified by law, the affected subjects are: individuals or also legal entities as in the case of Trust Services or in the case of electronic communication services[2]).

Next figure lays down a summary representation for the present and next (GDPR, NIS) laws involving data breach notification obligations, with special focus on timing requirements and recipients of the notifications. The time periods reported in the figure show the timing notification requirement from when the controller (the company) has became aware of a data breach event, i.e. the case has been detected and the company has taken the decision it is a data breach according to the definition of the relevant applicable law.



[1] Set up ad management of the Health Data Records is a DPCM 178/2015 law obligation addressed to the Italian national and regional Health services involved bodies. Each citizen shall have its own Health Data Record comprising his/her "health history" in using the national/regional health services.
The Health Data Dossier is instead a "health history" of a patient in only one health center(hospital,...), there is no obligatory link between Health Data Record and Health Data Dossier.

[2] The subscriber of a publicly available electronic communication services can be a natural as well as a legal person.

The situation is quite varied and the overall picture shows the complexity that companies have to face when they are controllers for more than one of the specific services in scope of such laws.

For example: TelCo and ISP providers have to fulfill the data breach obligations applicable for their publicly available electronic communication services but at the same time, for their internal Human Resource administration services, they have to respect the data breach notification obligations set out by the GDPR (enforceable by 2018).

Further example: on line search engine service providers and cloud services providers are among the addressees of the NIS data breach requirements (to be transposed by 2018 into the 28 European national legislation frameworks), therefore in case of incident impacting on the continuity of their services they have to notify the NIS Competent Authority or CSIRT[3] without undue delay and at the same time, whether personal data are affected, they have to notify the DPA without undue delay and then, according to the GDPR data breach notification obligations, notify again the DPA within 72 hours, and the affected subjects without undue delay whether it is likely to result in high risk the rights and freedoms of individuals.

Furthermore, if a breach of biometric data, used as authentication factor for accessing a company information system, then involves also personal data breach for the data processed, the same company toward the DPA will make a 24 hours notification for the biometric data and a separate 72 hours notification for the breach of personal data, with the consequent and well evident complexity in treating the case both for the company and the DPA.

Due attention to the necessary compliances should be taken also in consideration of the consequences in case of infringements:

- based on the privacy law in force, in Italy the violation of the data breach notification obligations in the electronic communication sector is sanctioned up to 150.000 eur in case of violation of data breach notification to the DPA and up to 1.000 eur for each subscriber or individual to whom the notification fails to be made or is delayed (article 162-ter of the Privacy Code). For the other cases of specific services (biometric data, Health Data Dossier) the sanction in case of infringement is up to 180.000 eur (violation of DPA Measures, article 162 of Privacy Code)
- according to the sanctions provided for the next European GDPR the applicable administrative fines are strongly increased:
    - up to 10 million eur, in case of undertaking up to 2% of the total worldwide annual turnover, whichever is higher) for infringement of provisions concerning notification of data breach to the DPA,
    - up to 20 million eur, in case of undertaking up to 4% of the total worldwide annual turnover, whichever is higher) for infringement of provisions concerning notification of data breach to the data subjects.

Hopefully, such composite framework of data breach obligations and related sanctions should be simplified/harmonised by appropriate regulatory actions in order to limit the data breach responsibility, and related efforts provided by all the parties, to the strictly necessary avoiding unreasonable burdens.

In any case companies should start to design and implement their own data breach management strategies in order to manage the relevant multiple data breach cases, ensuring fulfillment of the applicable law obligations in a controlled and cost- effective way.

[3] Competent Authority and CSIRT are entities with roles and responsibility set out by the NIS Directive.