

# Data protection and GDPR

## 1. Introduction

The growing interest in the instruments provided by the digital technology, and by Internet in particular, assumes considerable value by an economic and a sociological point of view. The future and the success of the diffusion of e-commerce in the European market will be determined by belief in or distrust of the Net by its users. There is a widespread fear of the new; psychological elements, such as the mistrust and the lack of confidence, represent serious obstacles to the approach to the electronic markets by the new users.

The advent of computers required adoption of specific means to safeguard personal information. The problem was to prevent the risks coming from the ease of collating and processing citizen's personal data. The digital revolution requires even the change of the notion itself, as well as of the contents, of the right of privacy.

The regulation of the relationships among the users of the electronic networks is a pivotal point for a well-balanced development of this important business sector. People have to bear in mind that Internet has not only a visible dimension, but also an invisible one.

## 2. Data Protection Principles

Data protection regulations in the European Union set the main principles that establish how data processing shall be performed. The most important privacy principles are summarized as follows:

- **Fair and Lawful Processing:** the collection and processing of personal data shall neither unreasonably intrude upon the data subjects' privacy nor unreasonably interfere with their autonomy and integrity and shall be compliant with the overall legal framework.
- **Consent:** personal data shall be collected for specified, lawful and legitimate purposes and not processed in ways that are incompatible with the purposes for which data have been collected.
- **Minimality:** the collection and processing of personal data shall be limited to the minimum necessary for achieving the specific purpose. This includes that personal data shall be retained only for the time necessary to achieve the specific purpose.
- **Minimal Disclosure:** the disclosure of personal data to third parties shall be restricted and only occur upon certain conditions.
- **Information Quality:** personal data shall be accurate, relevant, and complete with respect to purposes for which they are collected and processed.
- **Data Subject Control:** the data subject shall be able to check and influence the processing of his personal data.
- **Sensitivity:** the processing of personal data, which are particularly sensitive for the data subject, shall be subject to more stringent protection measures than other personal data.
- **Information Security:** personal data shall be processed in a way that guarantees a level of security appropriate to the risks presented by the processing and the nature of the data.

## 3. Consent of GDPR

Consent in the context of the GDPR refers to the assent or agreement by the data subject in relation to their personal data for the proposed processing activities associated with one or more entities. Given consent refers specifically to the form of consent given by the data subject in relation to their personal data and the proposed usage by activities (Ross, 2017). Consent can be considered to be an agreement between the data subject and the data controller (or other entity) and can therefore benefit from the same approach for implementing the data sharing agreements. This provides consistency in technology as well as encourages adoption of uniform standards and interoperability in dealing with similar use-cases.

For example, in cases where the consent is acquired through a web-form (Fatema et al., 2017), the entire webpage may need to be preserved to demonstrate that the consent acquisition process was in accordance with the conditions under the GDPR. Therefore, while the given consent may be represented in any form, it also has to somehow be linked to the processes responsible for acquiring the consent.

Additionally, any revision of consent data such as when updating or revoking consent also needs to be stored in a way that can be linked to the processes involved in the change as well as linked to the original consent. This is important as a matter of compliance as GDPR enforcement may require demonstration that a change in consent was carried out correctly, which is only possible through an introspection of what the original and changed versions of the consent are. This also introduces the dependency-like relation between data processes and consent where consent should be inherently linked to the processes that depend on it. For example, if the process of using personal data to send emails is dependent on the consent obtained from the user at the time of registration, then it is vital to show that the two are linked together, i.e., the emails are only sent based on the given consent. Such a system must also be able to demonstrate that updated consent has immediate effect on the processes that depend on consent.

#### 4. Conclusion

Since privacy in the digital context can be really guaranteed only if security standards are implemented, the study on the standard production process represents a pivotal point in the field of data protection. People need to become aware of the dynamics that drive to the elaboration of the technological standards governing the digital architecture.

People approach to the digital world is influenced by their expectations from digital networks. These expectations will shape the design of the digital environment in the near future. The next step is to incorporate values, principles, and codes of conduct inside the designs, in order to make clearer the necessary interaction between the technology development and the aims pursued by people legal systems.

## References

1. W. STALLINGS, Network Security Essentials. Applications and Standards, 3rd ed., Upper Saddle River, New Jersey, 2007, 19-22.
2. P. Guarda, Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks, 1<sup>st</sup>. ed., December 2008
3. G. PASCUZZI, Il diritto dell'era digitale, 2nd ed., Bologna, 2006.