

TITULO: Data Protection Regulation (GRDP and LOPDGDD)

HORAS: 57

GENERAL DESCRIPTION

This training action will provide students with the necessary skills to manage the regulations regarding data protection, as well as knowing the obligations of the person in charge and / or those responsible for processing them. They will also know the scope of these regulations and the penalty system.

GENERAL OBJECTIVES OF THE COURSE

- Knowing the current regulations governing the right to data protection, as well as the body that ensures compliance.
- Distinguishing the obligations of the person in charge and / or data processors.
- Knowing the regulations regarding data protection and guarantee of digital rights.
- Mastering the General Data Protection Regulation.
- Identifying the scope of the regulations.
- Describing the different types of rights with respect to data: right of access, rectification, cancellation and opposition.

CONTENTS:

LEARNING UNIT 1. LEGAL FRAMEWORK ON DATA PROTECTION IN SPAIN

1. Background
 - 1.1. Fundamental right
 - 1.2. The LOPDGDD (“Ley Orgánica de Protección de Datos Personales y Garantías de los derechos digitales” / Organic Law for the Protection of Personal Data and Guarantees of Digital Rights).
2. Approval and publication of the European Data Protection Regulation
 - 2.1. European context in the face of data protection

LEARNING UNIT 2. THE GENERAL REGULATION OF DATA PROTECTION OF EUROPE

1. Scope of application
 - 1.1. Territorial scope of application
 - 1.2. Non application of the GRDP
2. Definitions
3. Video surveillance
 - 3.1. Considerations regarding video surveillance in general
 - 3.2. Installation and recording of cameras
 - 3.3. Posters

LEARNING UNIT 3. REGULATED PRINCIPLES IN THE GENERAL REGULATION OF DATA PROTECTION

1. Principles related to treatment
 - 1.1. Lawfulness, loyalty and transparency of treatment
 - 1.2. Limitation of the purpose
 - 1.3. Data minimization
 - 1.4. Accuracy of the data
 - 1.5. Limitation of the term of conservation
 - 1.6. Integrity and confidentiality

LEARNING UNIT 4. LEGITIMATION

1. The consent. Terms
2. The informed consent: purpose, transparency, conservation, information and communication duty to the interested party
 - 2.1. Treatment manager
 - 2.2. Information
3. Consent of minors
4. Special data category
5. Data related to offenses and criminal penalties
6. Treatment that does not require identification
7. Legal bases other than consent

LEARNING UNIT 5. RIGHTS OF THE INTERESTED PARTY

1. Transparency and information
2. Right of access
 - 2.1 Way to attend to the right of access
3. Right of rectification
4. Right of abolition (right to be forgotten) Way to attend to the right
 - 4.1 Exceptions to the right of abolition
 - 4.2 The right of being forgotten on the Internet
 - 4.3
5. Right of portability Main elements
 - 5.1 Way to attend to the right
 - 5.2
6. Right of opposition and individualized decisions
7. Limitation of the treatment
8. Common aspects in the exercise of rights Rights of the interested party
 - 8.1
9. Exceptions to the rights
 - 9.1 Limitations and exceptions

LEARNING UNIT 6. ENFORCEMENT MEASURES

1. Data protection policies
 - 1.1. Actions and/or procedures
2. Legal position of the participants
 - 2.1. Responsible and co-responsible
 - 2.2. Managers, sub-managers of treatment
 - 2.3. Formalization of relations between responsible and manager
 - 2.4. Representatives of those responsible or managers for the treatment not established in the union.
- Registration of treatment activities

- 3.1. Registration of treatment activities as Responsible
- 3.2. Registration of treatment activities as a treatment manager
- 4. Provisions applicable to specific treatments.
 - 4.1. Treatment of contact data, entrepreneurs, individuals and liberal professionals.
 - 4.2. Credit information systems.
 - 4.3. Treatments for video surveillance purposes.
 - 4.4. Advertising exclusion systems.
 - 4.5. Information systems of internal complaints.
 - 4.6. Processing of data related to infractions and administrative sanctions

LEARNING UNIT 7. PROACTIVE RESPONSIBILITY

- 1. Risk assessment
 - 1.1. Information gathering
 - 1.2. Data processing
 - 1.3. Information dissemination
 - 1.4. Invasive acts
- 2. Privacy from design and default: Fundamental principles
 - 2.1. Preventive protection. Proactivity
 - 2.2. Privacy “by default”
 - 2.3. Privacy integrated in the design: “in the DNA”
 - 2.4. Full functionality “win-win” instead of “plus zero”
 - 2.5. Protection throughout the life cycle: “End to end”
 - 2.6. Visibility and transparency: “Trust but Verify”
 - 2.7. Empowerment of the user. The user in the centre: “User – centric”
- 3. Impact assessment related to data protection and prior consultation. High risk treatments
- 4. Security breaches. Notification of security breaches
- 5. The data protection delegate
- 6. Codes of conduct and certifications

LEARNING UNIT 8. THE DATA PROTECTION DELEGATE

- 1. Mandatory designation
 - 1.1. Main activities of the Responsible
 - 1.2. Large scale
 - 1.3. Regular and systematic monitoring
 - 1.4. Special categories of data and data relating to convictions and criminal offenses
- 2. Skills of the Data Protection Delegate
 - 2.1. Knowledge level
 - 2.2. Professional qualification
 - 2.3. Ability to perform their tasks
 - 2.4. DPD based on a service contact information
- 3. Publication and communication of the contact data of the data protection delegate
- 4. Position of the data protection delegate
 - 4.1. Involvement in all issues related to data protection
 - 4.2. Necessary resources
 - 4.3. Instructions and “Independent acting”
 - 4.4. Dismissal or penalty for performing DPD tasks
 - 4.5. Conflict of interest

5. Functions of the data protection delegate
- 5.1. NGPD compliance control
- 5.2. The role of the DPD in an impact assessment of data protection
- 5.3. Risk based approach
- 5.4. The role of the DPD in maintaining records

LEARNING UNIT 9. SUPERVISORY AUTHORITIES

1. Supervisory authority
 2. Powers of the supervisory authorities
 3. European data protection committee
 4. Penalty system
 5. Procedures of the supervisory authorities
 6. Jurisdictional guardianship
 7. The right of compensation
 8. Process of adaptation to the European General Regulation on Data Protection
 - 8.1. Identification of the legal basis of the performed treatments
 - 8.2. Verification of the information provided to interested parties
 - 8.3. Establishment of a record of treatment activities
 - 8.4. Stakeholder rights exercise
 - 8.5. Identification of security measures
 - 8.6. Verification of relationships with treatment managers
-
9. International transfers