PROGRAM CUORE | Employee Support
Continuous Training

Program I:

General Fundamentals of Data Protection and Information Security

Gi Group HOLDING

Welcome to your Training

In connection with your Employment Contract, GI GROUP hereby sends its **Employee Training Program**.

This training is mandatory and corresponds to the initial training modality, which we consider to be an added value, both for your personal and professional development and for raising awareness of the guiding principles of this Module, considered to be of greatest relevance in ensuring professional excellence.
These courses are organized as distance learning and, in the self-training modality, an individual learning modality that allows the individual to learn at their own pace, using specific resources for this purpose, and which contributes to the increase of their personal and professional skills without the need for continuous monitoring by a tutor or trainer.

By accessing this Module, the Employee declares that he/she undertakes to:
1. Access the training material and dedicate the necessary time to develop your skills and complete this Module;
2. Do not transmit the training materials received to third parties, in any form.

If you need support, please contact: formacao.colaborador@gigroup.com

Program Content

The importance of Confidentiality and Privacy
Data Protection Culture
General Data Protection Regulation (GDPR):
- Legal Framework
- Applicability

Definitions
- Personal data
- Data Processing
- Fundamentals for Data Processing

Guiding Principles of the Law
Data Subject Rights
Personal Data Breach
Information Security
- Basic concepts
- Information Classification and Labeling
- Secure Information Transmission

Training Debriefing – Lessons Learned

The importance of Confidentiality and Privacy

Confidentiality

Confidentiality guarantees that information is accessed only by people who have authorization to do so, respecting the rules established in this regard.

Confidential information must not be used for your own benefit or that of third parties and no information may be disclosed that has not been previously authorized.

Examples of Confidentiality content:

- **Personal data;**
- **Financial information;**
- **Strategic and commercial plans;**
- **Contracts;**
- **Fusions and acquisitions;**
- **Technical specifications, among others.**

The importance of Confidentiality and Privacy

Privacy

Privacy is a concept associated with confidentiality and which includes the protection of information available, with the aim of ensuring compliance with applicable legal standards and the fundamental right of each individual to decide who should have access, at any given time, to their data.

Failure to comply with all standards and good practices in personal data privacy may:

- Constitute a violation of the rights provided for in the Personal Data Protection Law (Law 67/1998) and the General Regulation on Data Protection (679/2016 of the EU).Constitute an illicit act, subject to disciplinary, civil and/or criminal sanctions.
- Seriously compromise the Company's image and reputation.

Data Protection Culture

Below we present some suggestions so that you can actively contribute to promoting a culture of data protection, from your workplace:

1. If you are not at your workstation, ensure that you remove all paper documents from your desk or other locations (printers, fax machines, etc.) to prevent unauthorized access.
2. Whenever you are absent from your work station, ensure that you block access to your computer or other equipment that processes personal data.
3. Your computer screen must not allow viewing or unauthorized access to information considered restricted and/or sensitive.
4. Do not share your password or access credentials. All passwords are viewed as confidential data.
5. The file containing restricted and/or sensitive information must be kept reserved and closed whenever it is not in use.

General Data Protection Regulation (GDPR)

Legal Framework

- 1995 – The European Union approves the Personal Data Privacy Directive.
- Apr. 2016 - The European Union approves the General Data Protection Regulation (GDPR), a substantive review and strengthening of the European Union's privacy principles - to come into force in May 2018.
- Jul. 2016 -EU-US announce the replacement of the now defunct Safe Harbor: the EU-US Privacy Shield Framework (mechanism that guarantees the cross-border flow of data from the EU to Outside the EU).
- The General Regulation on Personal Data Protection (EU Regulation 2016/679) will be applied directly in all EU Member States from May 25, 2018, replacing the directive in force to date.

General Data Protection Regulation (GDPR)

Applicability

The General Data Protection Regulation (GDPR) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and the free movement of such data, revokes the previous Directive 95/46/EC and represents legislation aimed at harmonizing data privacy laws across Europe.

Application of the GDPR to all public and private entities.

Applicable to data processing carried out in the European Union and outside the European Union.

Definitions

Personal data

For the purposes of current legislation, personal data is understood as any information of any nature and regardless of its support, including sound and image, relating to an identified or identifiable natural person (“data subject”). A person who can be identified directly or indirectly, based on a given piece of data, is considered identifiable.

Some examples:

- Name
- Identification number
- Connection cookies
- Physical, physiological, genetic, mental, economic, cultural or social identity of the natural person, among others.

Definitions

Personal Data * *New*

The GDPR now includes:

Location Data

Consumers carrying their smartphones or tablets may not realize how much geolocation data is being captured or what is being used.

Electronic Identifiers

Personal data now includes email addresses, information about internet browsing habits, IP addresses, cookies, among others.

Definitions

Data Processing

An operation or set of operations carried out on personal data, by automated or non-automated means, such as collection, registration, organization, structuring, conservation, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, broadcast or any other form of availability, comparison or interconnection, limitation, erasure or destruction.

Definitions

Data Processing – Fundamentals

For the processing of personal data to comply with the Law, one of the following grounds must be verified:

- **Consent of the Data Subject (free, informed, express and written);**
- **Contractual obligation (execution) or pre-contractual measures, at the request of the Data Holder;**
- **Legal obligation to which the Data Controller is subject;**
- **Defense of the vital interests of the Data Subject or another natural person;**
- **Public interest;**
- **Legitimate interest pursued by the Data Controller or third parties.**

Guiding Principles of the Law

Principle of lawful, fair treatment and transparency.

Companies need to ensure that their practices, processes and internal data processing systems are based on fairness and transparency of treatment. We reinforce the need to consult the GI GROUP Privacy Statement so that you know in detail our guidance at this level.

Principle of specification and purpose limitation.

Companies must collect and process personal data, depending on a specific purpose. Likewise, the data must be reserved for the time strictly necessary, considering this purpose.

Principle of data minimization.

Companies must only process personal data considered necessary to achieve their processing objectives.

- ✓ Lawful, fair and transparent treatment
- ✓ Purpose limitation
- ✓ Data minimization
- ✓ Data accuracy
- ✓ Data conservation
- ✓ Security and Confidentiality

Guiding Principles of the Law

Principle of data accuracy.
The Regulation states that “every reasonable step must be taken” to erase or rectify data that is inaccurate or incomplete. Data Subjects have the right to request that inaccurate or incomplete data be erased or rectified.

Principle regarding data conservation.
Companies need to develop internal mechanisms for deleting personal data, when they are not necessary, safeguarding their conservation for the strictly necessary period.

Principle of security and confidentiality.
Personal data must be “processed in a way that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures”.

- ✓ Lawful, fair and transparent treatment
- ✓ Purpose limitation
- ✓ Data minimization
- ✓ Data accuracy
- ✓ Data conservation
- ✓ Security and Confidentiality

Data Subject Rights

Right to Information: The Data Subject has the right to receive the information necessary for their knowledge and clarification regarding the privacy policy applicable to their processing.

Right to Access: The Data Subject has the right to access the information that the Company/Entity holds about them.

Right to Edit/Rectify: The Data Holder has the right to request the alteration or rectification of their personal data, with a view to updating their information.

Right to Object: The Data Holder has the right to object to the collection and/or processing of their data for marketing and advertising purposes.

Right to be Forgotten: The Data Holder has the right to request the deletion of their personal data from the Company/Entity's systems.

Right to Portability: The Data Holder has the right to request, in an accessible file, the personal data transmitted and held by the Company/Entity.

- ✓ The response to the Data Subject is mandatory and must occur within 30 days after the initial request.
- ✓ As a Data Holder, if you need to exercise any of the rights provided, we ask that you contact Consultant GI GROUP directly or, alternatively, via the address: pt.privacy@gigroup.com

General Data Protection Regulation (GDPR)

Personal Data Breach

The new regulation requires that, by default, new goods, services, products, systems, devices and processes are built, from the development phase, in accordance with privacy and protection requirements (privacy by design). , in order to guarantee maximum protection of information.

Personal Data Breach: what is it? It means, first and foremost, a security breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data. It's more than just losing personal data.

Personal Data Breach: Some examples:

- Access to personal data by people not authorized to do so;
- Deliberate or accidental action by the Data Controller or Subcontractor;
- Sending information with personal data to incorrect recipients, among others.

Whenever you become aware of any situation that could be recognized as a “Personal Data Breach”, you must immediately report it to GI GROUP, via: pt.privacy@gigroup.com

General Data Protection Regulation (GDPR)

Information Security

Information can exist in various formats: printed, electronically stored, verbal, transmitted by conventional mail...

It is the responsibility of information security to protect it from various types of threats, to ensure business continuity and minimize risks.

Information security comprises the protection of information, systems, resources and other assets against disasters, errors, and unauthorized manipulation.

Therefore, information security must also be applied at all stages of the life cycle in the activities carried out daily.

Why should you care about information security? Most common problems:

- Destruction of information and other resources
- Modification or misrepresentation of data
- Theft, removal or loss of information
- Information disclosure
- Service interruption

General Data Protection Regulation (GDPR)

Information Security – Basic Concepts

Information Asset: Information is an essential element for all the organization's business processes, and is therefore a good or asset of great value
Vulnerability: These are the weaknesses present in information assets, which can cause, intentionally or unintentionally, the breach of one or more of the three principles of information security: confidentiality, integrity, and availability
Threat: The threat is an agent external to the information asset, which, taking advantage of the vulnerabilities of this asset, may break the confidentiality, integrity or availability of the information supported or used by this asset
Probability: The probability is the chance of a security breach occurring taking into account the degree of vulnerabilities present in the assets that support the business and the degree of threats that could exploit these vulnerabilities.
Impact: The impact of an incident is the potential consequences that this incident may cause to the organization's business and others involved
Risk: Risk is the relationship between probability and impact. It is the basis for identifying points that require investment in information security

People are the central element of an information security system.
Information security incidents almost always involve people, either on the side of the exploited vulnerabilities or on the side of the threats that exploit these vulnerabilities.
Stay alert and ensure maximum compliance with the procedures and practices established in your workplace in this context.

General Data Protection Regulation (GDPR)

Information Classification and Labeling

Information Holders are responsible for classifying the information they create or acquire according to the data classification standards in force in the companies in which they are located.

- The Holders are then responsible for ensuring that access to such information is managed based on the standards established by such Entities.
- Information Subjects must work with appropriate support functions, such as IT, to ensure that appropriate controls are maintained to limit access to information based on the principle of necessity.
- Information Holders are responsible for ensuring that their documents are maintained in accordance with the Records Retention Plan in force at the Entity.

All Employees are responsible for remaining aware of vulnerabilities and threats, such as social engineering, interface mystification (phishing) and other attacks/exploits, and for protecting themselves from unauthorized access and use of the Information Systems they use. interact professionally.

Employees who violate such procedures may be subject to disciplinary measures that may lead to the termination of the employment contract and the initiation of civil or criminal proceedings.

General Data Protection Regulation (GDPR)

Information Classification and Labeling

Classification of Confidential Information
information that the Company has a legal obligation to keep confidential or that should be considered commercially or competitively sensitive information.

Personal, Commercial, Financial, Proprietary Data:

- **Access:** Viewing and editing access will only be granted to employees who need it to perform their work.
- **Transfer:** Users must take proactive measures to protect the transfer; for example, use approved encrypted file transfer methods, avoid electronic messages whenever possible, and never send information to a recipient who does not require such information.
- **Storage:** Users must store physical documents in closed locations. Electronic data must be stored in secure locations, such as approved cloud storage or approved network storage with appropriate access controls

Furthermore, subsets of Confidential Information may also be regulated or controlled under legislation, sectoral standards or commercial agreements. The Company may impose additional processing requirements in relation to such data, consistent with the requirements established by the competent authority. Stay alert and look for relevant information in this area, in your workplace.

General Data Protection Regulation (GDPR)

Information Classification and Labeling

Classification of Internal Information
Company Information that is not Confidential or Public.

Intranet pages, Email, Newsletters/Memos

- **Access:** Access to viewing and editing will be limited to groups of people based on their department or job classification.
- **Transfer:** Users must take proactive measures to protect the transfer; although it may be sent with reasonable precautions whenever applicable and possible.
- **Storage:** Information can be stored in secure locations, such as lockable cabinets or user hard drives.

Furthermore, subsets of Confidential Information may also be regulated or controlled under legislation, sectoral standards or commercial agreements. The Company may impose additional processing requirements in relation to such data, consistent with the requirements established by the competent authority. Stay alert and look for relevant information in this area, in your workplace.

General Data Protection Regulation (GDPR)

Information Classification and Labeling

Classification of Public Information
information whose unauthorized disclosure, alteration or destruction would cause little or no risk to the Company

External Website, Press Releases, Marketing Materials

- **Access:** Viewing access can be freely granted. Access to editing must continue to be controlled by the Information Holder.
- **Transfer:** Users must take proactive measures to protect the transfer; although it can be sent freely by any means.
- **Storage:** Information can be stored wherever necessary, unless otherwise stipulated by the company.

Furthermore, subsets of Confidential Information may also be regulated or controlled under legislation, sectoral standards or commercial agreements. The Company may impose additional processing requirements in relation to such data, consistent with the requirements established by the competent authority. Stay alert and look for relevant information in this area, in your workplace.

General Data Protection Regulation (GDPR)

Secure Information Transmission

- Users will not use their Company-assigned laptops, desktops, or mobile devices (if applicable) to download or store large volumes of personal photos, songs, files, or other non-work-related data and applications. Neither GI GROUP nor the Company you work for will be responsible for the loss of any such data.
- Users will not use Company-assigned devices (if applicable) to receive large-volume video or audio transmissions or to use hot-spotting technology for personal use.
- Outlook's Information Rights Management (IRM) permissions must be used whenever Confidential Information is transmitted by email. IRM enables users to encrypt a message and specify access permissions to prevent unauthorized persons from reading, printing, forwarding or copying sensitive information.
- The introduction of unauthorized devices into the global corporate network creates a security risk or a potential disruption of the technological infrastructure, if not authorized.

We summarize the main results achieved through this training:

1. Know how to identify behaviors to adopt, in order to guarantee the Confidentiality and Privacy of information
2. Know how to understand the concepts associated with Data Protection and Security
3. Know how to identify the Guiding Principles of the Law (GDPR), within the scope of the data processing flow
4. Know how to recognize potential personal data breach situations and how to report them, with a view to resolving them.
5. Know how to work in the context of information security, with regard to access, transfer and storage of data

Now that you have completed this action, access the **knowledge assessment questionnaire HERE (Mandatory step for completing this action).**