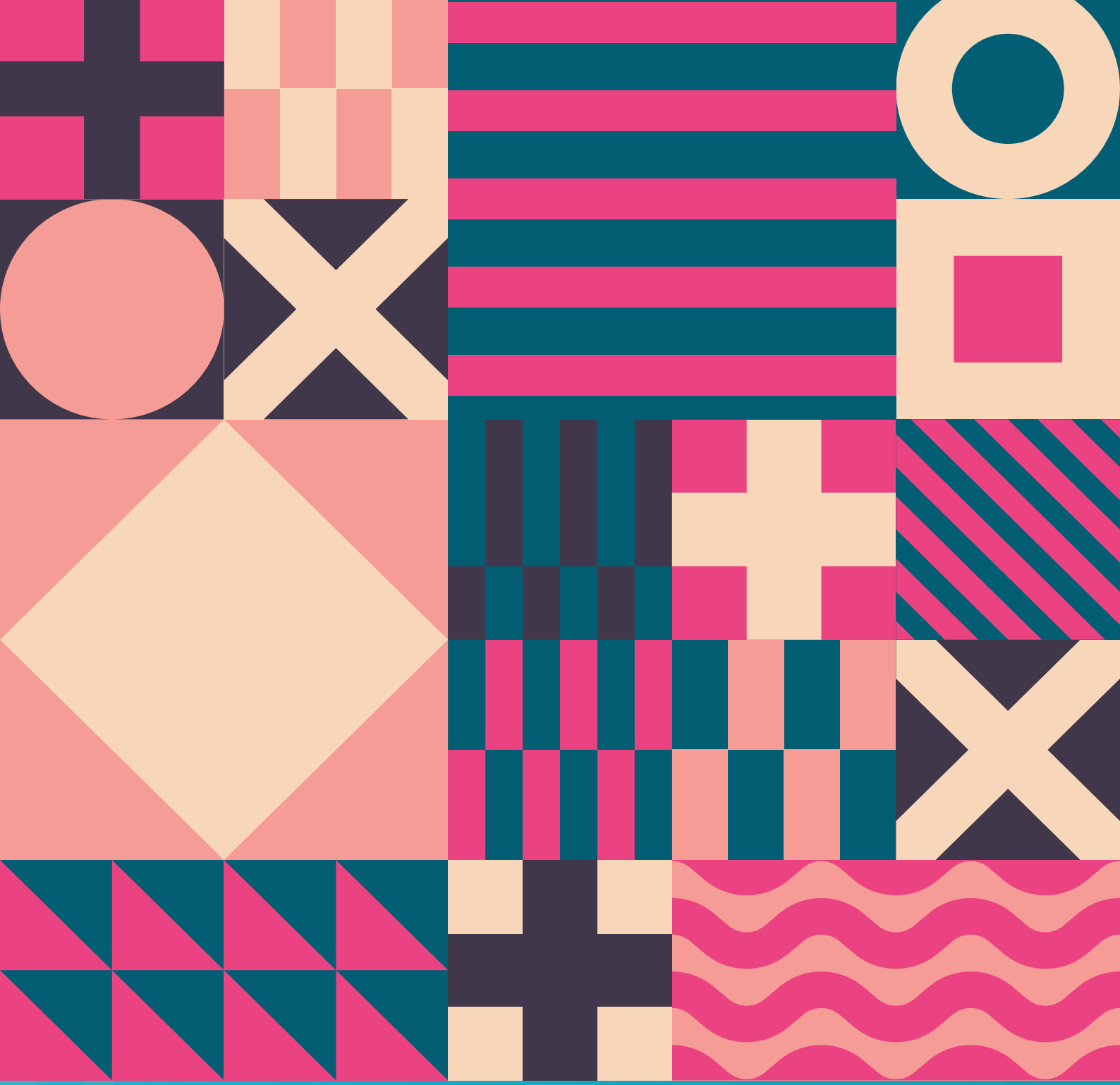

# Manual of Best Practices Regarding the Application of the General Data Protection Regulation

ISTEC INSTITUTO SUPERIOR DE TECNOLOGIAS AVANÇADAS DE LISBOA

SIGQ_RGPD_MBP_R1_0523

# Índice


Introduction 3
Areas of use of personal data 4
1. Academic Management 4
2. Scientific research 4
3. Video surveillance 5
4. Rendering of Services to the Community 5
5. Alumni 5
6. Events and other initiatives 6
7. Institutional Communications 6
8. Student Card 6
9. Technological Infrastructures 6
10. Cookies 7
11. Administrative Management 7
Best Practices in Data Handling by Area 7
1. Academic Services 8
1.1. Keep data for future contact (e.g.: disclosure of training offer) 8
1.2. Collecting personal documents 8
1.3. Receipt of personal data when registering 8
2. Financial Services and Treasury 9
2.1. Collection of Employees' Data 9
2.2. Collecting personal documents 9
3. Communication and Public Relations Office 10
4. Student Support and Employability Office 11
5. Office of Educational Projects and Internationalization 12
6. Internal Quality Office 13
7. Information Technology and Systems Office 13
7.1. Computer and computer network access 13
7.2. Access to software and institutional e-mail accounts 13
7.3. Security Copies 14
Security and Privacy Best Practices 15
1. Privacy and Personal Data Protection 15
2. Electronic Mail 16
2.1. Email account forwarding 16
2.2. Check Recipients 16
2.3. Attachments to messages 16
2.4. Critical and personal information 17
2.5. Disclaimer 17
3. Clean Table Policy and Use of Equipment 17

# Introduction

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the GDPR), came into effect on 25 May 2018, emphasizing the protection of individuals to the processing of personal data as a fundamental right.
The RGPD, in Art. 1 (object and objectives), point 1, "... lays down the rules relating to the protection of individuals about the processing of personal data and the free movement of such data.", in point 2, "this Regulation upholds the fundamental rights and freedoms of individuals, and in particular their right to personal data protection."

ITA - Instituto de Tecnologias Avançadas para a Formação, Lda, as the instituting body of ISTEC Lisbon - Instituto Superior de Tecnologias Avançadas de Lisboa, is committed to ensuring the privacy of personal data received and stored in its databases.
Accordingly, ISTEC Lisbon's Privacy Policy establishes that information of a personal nature is treated and protected with all the diligence and care that data processing requires, following Regulation (EU) 2016/679, RGPD.

ISTEC Lisbon is strongly committed to the protection of personal data and the respect for the exercise of the right to privacy of its users. To assist the whole academic community and interested parties in the implementation of good practices regarding the application of ISTEC Lisbon's Privacy Policy and the GDPR, by creating this manual which defines concrete measures and practices to safeguard personal data.

This manual of best practices regarding the application of the General Data Protection Regulation was developed to provide clear and practical guidelines to protect the security and privacy of personal data in our increasingly connected digital environment. As we move into the digital transition era, we must take effective measures to protect our systems, personal information, and the confidentiality of data.

# Areas of use of personal data

In higher education, the use of personal data plays a key role in several areas, contributing to the improvement of teaching quality, the advancement of scientific research and the personalization of the experience for students.
The collection and processing of personal data at ISTEC Lisbon occur in an ethical, transparent manner and compliance with the General Data Protection Regulation (2016/679) and following ISTEC Lisbon's Privacy Policy.

The areas where data is collected, processed, and used are:

## 1. Academic Management

To provide us with the necessary conditions to build an academic path and ensure compliance with all legal obligations to which we are subject, your data will be processed for the following purposes:

a. Enrolment and enrolment management.
b. Maintenance and updating of the individual student file.
c. Granting of special attendance statuses.
d. Management of mobility programs of national and/or international character.
e. Recognition of equivalences and documents conferring degrees and other academic titles.
f. Issuing certificates and diplomas.
g. School insurance maintenance and claims reporting.
h. Administrative management of DGES scholarships.
i. Management of attendance, grades, and other academic information.
j. Management of other social support.

## 2. Scientific research

In the context of its mission as a higher education institution, ISTEC Lisbon assumes as one of its main objectives the promotion of scientific research, aiming not only at the production and disclosure of knowledge but also at the enhancement of the activity of its teachers, researchers, and students.

In this context, you may be asked to collaborate on projects promoted by members of ISTEC Lisbon's academic community within the scope of their respective study cycles or research activities. The specific data to be collected and the purpose of its collection will depend on the research project in question, as well as the format of the study itself. In any case, your participation will always be voluntary, and your data will only be processed with your consent, in strict compliance with the ethical standards recognized by the scientific community and under ISTEC Lisbon's Code of Ethics and Conduct.

## 3. Video surveillance

To ensure your safety and that of all those who interact with us, as well as that of the assets located within our perimeter (Lumiar Academic Campus), whether they belong to ISTEC Lisbon or third parties, ISTEC Lisboa has Video Surveillance Systems at various points within its premises.

All cameras are installed in strict compliance with the legal requirements.

## 4. Rendering of Services to the Community

Through ISTEC Lisbon and the Advanced Computing Research Unit (UICA), or structures specially set up for this purpose, ISTEC Lisbon makes its knowledge available to the community, in the form of services provided in various fields of knowledge, with special emphasis on the area of information technologies.
In this sense, you will have access to laboratories, classrooms, lecture rooms, and auditoriums, among others.

The personal data you provide in this context will be used solely and exclusively to provide the services you request, as well as, given the Institute's mission, to ensure the training of its students and promote scientific research.

## 5. Alumni

In addition to other communications that you may eventually subscribe to, you will be sent, via e-mail, communications related to:

a. ISTEC Lisbon news.
b. Alumni professional success initiatives (publications, books, blogs, positions, television programs, etc.).
c. Employability surveys.
d. Publicizing professional opportunities.
e. Continuing education offers.
f.Events specifically targeted to the alumni audience.

You may at any time, without the need to justify, unsubscribe from receiving such communications.

## 6. Events and other initiatives

Within the scope of initiatives promoted by ISTEC Lisbon (Workshops, Seminars, Conferences, Job Fairs, etc.), some of your personal data may be requested to manage your registration and accreditation, as well as billing (in case of paid events).

Additionally, photographs and/or videos may be taken for disclosure and promotion in internal and external communication channels.

## 7. Institutional Communications

To make known the activities developed by ISTEC Lisbon and inform you about the life of the Institute and the different bodies belonging to the academic community, you may receive different types of communications, such as:

a. Newsletters.
b. Disclosure of the Institute's training offer.
c. Disclosure of professional opportunities.
d. Disclosure of information from the Scientific-Technical Council, Pedagogical Council and Student Ombudsman.
e. Disclosure of initiatives from the Students Association of the Institute of Advanced Technologies of Lisbon (AEISTEC).
f. Requests for collaboration in scientific research activities.

## 8. Student Card

A partnership with Caixa Geral de Depósitos resulted in, ISTEC Lisbon Student Card is your identification document as a member of the academic community, granting you access to a wide range of services of the Institute and partner institutions. For more information on the Privacy Policy and Protection of Personal Data of Caixa Geral de Depósitos, please visit this link:
https://www.cgd.pt/Ajuda/Pages/Politica-Privacidade-Protecao-Dados-Pessoais.aspx

## 9. Technological Infrastructures

With the use of ISTEC Lisbon's technological infrastructures, including Wi-Fi networks, some of your data will be automatically collected and analysed to monitor the security of these infrastructures and prevent their abuse.

## 10. Cookies

you visit us. Cookies are small electronic files stored on your device that allow the platforms to distinguish each visitor and keep your preferences throughout your session. The cookies used by ISTEC Lisbon respect anonymity and will not be used to collect personal information.

On ISTEC Lisbon portals the Google Analytics service is used, with information stored in cookies kept by Google for statistical and search analysis purposes. For more information on the types of cookies used by Google, you can consult the privacy policies here: https://policies.google.com/privacy

## 11. Administrative Management

To ensure the regular operation of ISTEC Lisbon, some of your data may be processed to:

a. Support decision-making and the continuous improvement of internal processes.
b. Issuing the student ID card.
c. Control and management of access and use of ISTEC Lisbon services, such as the library, sports, and technological infrastructures, among others.
d. Payment processing.
e. Consideration of complaints, requests, appeals and similar procedures.
f. Management of election procedures.
g. Conducting audits and certification and accreditation procedures.
h. Completion, for communication to the Directorate General of Education and Science Statistics, of the RAIDES and RENATES surveys, among others.
i. Compliance with other legal obligations, including cooperation with the competent authorities.
j. Communications in case of possible emergencies.

# Best Practices in Data Handling by Area

The responsible and ethical handling of personal data at ISTEC Lisbon is an essential element to ensure the confidentiality, integrity, and privacy of information of students, faculty and other members of the academic community.

For each functional area, there is a set of good practices that must be observed, they are:

# 1. Academic Services

## 1.1. Keep data for future contact (e.g.: disclosure of training offer)

If there is a need to keep the data for future contact, the data subject's consent must be sought for this purpose.

If the data subject indicates that he/she does not want the personal data to be kept, the data provided must be deleted (the consequence of the refusal of consent), and an e-mail can be sent for this purpose.

## 1.2. Collecting personal documents

The collection of data such as the photocopy of the citizen ID card or any other identification document (card with NIF + Identity Card + Social Security Card) without consent of the individual, should not be accepted by Academic Services.

A stamp indicating "I authorize the copy of the document" with the date and signature of the data owner should be used.

If the data owner does not want to provide the document, he or she has the right to object, in which case a stamp should be placed that the data is in accordance with the original document, duly displayed and signed by the individual and the employee who handled this process.

## 1.3. Receipt of personal data when registering

The student is notified of the conditions of attendance in the course or study cycle in which he/she is enrolled, assuming full responsibility, under the terms of the law, for the accuracy of the data contained in this form.

General information:

a. Persons presenting themselves as family members or guardians of the student may only obtain information in the presence of the student, if the student is not present, only with a power of attorney signed by the student conferring powers to that effect.

b. The student's data, digitally obtained, must be organized by folders with reserved access and conditioned to the service manager, with access password and in its reserved area. The folders must not be stored on a desktop.

c. The students' physical files should not be consulted in front of third parties, and due confidentiality must be ensured.

d. The contact with the Foreigners and Borders Service (SEF) should be preceded by the written authorization of the individual so that the data provided to that Service (name, date of birth, nationality) for scheduling the visa extension, is covered by the rules contained in the RGPD.

e. When the lecturers are in the Academic Services area, the work in progress shall remain properly hidden from the lecturer, except if the lecturer requests information about a specific student, in which case the information shall be made available, but in a reserved way and limited to what is strictly necessary.

f. A "clean desk and equipment use policy" should be implemented and enforced, i.e., no personal data should be on display and with conditional access in the workspace.

g. Email address signatures should contain a confidentiality message.

## 2. Financial Services and Treasury

### 2.1. Collection of Employees' Data

The collection of the employee's data, such as an address, cell phone number, email address, name of spouse and dependents, and date of birth, among others, must be made in a form suitable for this purpose in paper format and filed in a locked cabinet and digitally archived, with password protection in an encrypted folder.

### 2.2. Collecting personal documents

The collection of data such as the photocopy of the citizen card or any other identification document (Fiscal Number Card + Identity Card + Social Security Card) without the consent of the data owner, should not be accepted by the Services.

A stamp indicating "Copy authorized by yourself" must be used on all documents where there is a reproduction.

If the individual does not allow this, a stamp that the data "conforms to the original document" should be placed on these documents and signed by the individual and the employee who handled this process.

General information:

a. The digitally archived data of employees (teaching and non-teaching staff) must be organized in folders with access restricted to the person responsible for the service, with an access password and in his/her private area. The folders must not be stored on a local desktop.

b. The digitally archived employee data must be organized in folders with restricted and conditioned access to the service manager, with access password and in his restricted area. The folders must not be stored on a local desktop.

c. The employees' physical files must not be consulted in front of third parties, and due confidentiality must be guaranteed.

d. The "clean desk and equipment use policy" should be implemented and enforced, e.g., personal data and conditioned access should not be exposed in the workspace.

e. Email address signatures should contain a confidentiality message.

## 3. Communication and Public Relations Office

The right to image is a right of personality, constitutionally enshrined and protected (Article 26.1 of the CRP).

The capture and/or disclosure of an image must be preceded by consent from, the individual must know the purposes of the use of his image and may oppose its processing, archiving, or disclosure, at any time. However, article 79.2 of the Civil Code states "The consent of the person portrayed is not necessary when this is justified by his/her renown, the position he/she holds, police or justice requirements, scientific, didactic or cultural purposes, or when the reproduction of the image is framed in that of public places, or in that of facts of public interest or that have taken place publicly. "Only in these cases may consent not be necessary, however, given the publication of the RGPD and the concerns exposed with this issue, namely because of social networks, the request for consent should always be requested and filed.

This request should be made to students, faculty, non-teaching staff, and others external to the organization (e.g., guests of lectures).

General information:

a. The processing of personal data involving the capture and collection of images or video requires the prior consent of those involved. The consent must be express, unequivocal, containing the purposes, namely where and how the image or video will be published, the identification of the event, the deadline for publication, and the right to object.

b. The photographs and videos must be destroyed after the deadline set for their publication and processing.

c. ISTEC Lisbon publicity containing the image or video of individuals must have the data owners' express consent. This type of publicity must have a shorter period of validity. The greater the exposure of the actors and data subjects, the shorter the duration of the advertising campaign should be.

d. Photographs taken at events organized by ISTEC Lisbon, or organized and held at the Lumiar Academic Campus, must not identify individual persons, without their prior consent. If this consent cannot be obtained, the photographs should be blurred to the point where the image does not allow the identification of the individual person or focus, alternatively, on people with their backs turned.

e. The disclosure of ISTEC Lisbon's training offers at high schools and vocational schools is particularly sensitive if the public present is minors. In this case, the authorization of the Guardians is required for the collection of personal data, without which it cannot be accepted, even if freely made available by the minor, any data or personal information.

f. Visiting cards requested by faculty and researchers and technical, administrative and management staff, with authorization, must be preceded by express consent if they express a wish to publish their private and personal mobile contact.

g. The publications on social networks where images are used, in the sharing of information or advertising campaigns, must not identify individual persons, without their prior consent. If this consent cannot be obtained, the photographs must be blurred to the point where the image does not allow the identification of the individual person or focus, alternatively, on people with their backs turned.

h. A "clean desk and equipment use policy" should be implemented and enforced, e.g., no personal data should be exposed and conditional access in the workspace.

i. Email address signatures should contain a confidentiality message.

## 4. Student Support and Employability Office

Incoming emails from partner companies, as well as information sent by students, should only be viewed by people who are part of the Student Support and Employability Office.

General Information:

a. When completing the interest survey on preferences in completing curricular internships, explicit and informed consent must be obtained from students prior to the collection, processing, or sharing of personal data. It must be ensured that students are aware of how their personal data will be used.

b. Only the personal data strictly necessary to fulfil the specific purposes of the office should be collected, avoiding the excessive collection of information, and ensuring that data retention is limited to the necessary period.

c. Provide students with clear and transparent information on how their personal data is handled, not only by ISTEC Lisbon but also by the partner companies when carrying out their curricular internships.

d. Ensuring that students can access their own personal data and, if necessary, correct or update it, establishing procedures so that students can exercise their right of access and rectification easily and efficiently.

e. Limit the sharing of personal data with third parties only for authorized purposes and based on an appropriate confidentiality and data protection agreement.

f. In the Workplace Training protocols carried out in compliance with the curricular internships of all ISTEC Lisbon courses, it must be ensured that clauses are included that expressly and unequivocally guarantee that students undertake not to disclose or transmit, directly or indirectly, to any third parties, data or facts of a confidential nature regarding the training company, its organization, its business, products, clients, strategies, procedures, equipment, manufacturing processes or activity by it this prohibition is in force both during the curricular internship and after its termination;

g. A "clean desk and equipment usage policy" should be implemented and enforced, e.g., personal data should not be exposed and with conditional access in the workspace.

h. Email address signatures should contain a confidentiality message.

## 5. Office of Educational Projects and Internationalization

The e-mails received from Foreign Institutions of Higher Education should only be seen by people who are part of the Office of Educational Projects and Internationalization.

General information:

a. The data entered in the National Agency System under the Erasmus + Program, should be made only by one person. Obtaining this information by email must observe the measures previously mentioned. The data must be treated in a way that guarantees the confidentiality of the data.

b. The "clean desk and equipment use policy" should be implemented and applied, e.g., no personal data should be exposed and with conditioned access in the workspace.

c. Email address signatures should contain a confidentiality message.

## 6. Internal Quality Office

The emails received from external institutions and the whole academic community of ISTEC Lisbon should only be viewed by the people who are part of the Internal Quality Assurance System Office.

General information:

a. Data collected through surveys should be anonymized (if applicable) before the disclosure.

b. A "clean desk and equipment use policy" should be implemented and enforced, e.g., no personal data should be exposed and with conditioned access in the workspace.

c. Email address signatures should contain a confidentiality message.

## 7. Information Technology and Systems Office

The Office of Information Technology and Systems, by inherent function, is ISTEC Lisbon's technical support unit, exercising its function in planning, implementation, management, support and promotion of the use of communications and computer services, and information systems.

### 7.1. Computer and computer network access

Access to personal data or data classified as sensitive, directly from computers or through ISTEC Lisbon's internal computer network, must be segmented with different levels of access, with the employee only having access to areas that are his or her responsibility, according to his or her duties and the need to access certain personal and/or sensitive data, and with security achieved through the definition of passwords provided to ISTEC Lisboa employees.

### 7.2. Access to software and institutional e-mail accounts

Access to personal data or data classified as sensitive, directly from a computer, or through ISTEC Lisboa's internal computer network or even those "housed" in billing, payroll management software, etc. and data that may eventually be found in ISTEC Lisboa's e-mail boxes, must be segmented with different levels of access, with the employee only having access to areas that are his or her responsibility, according to his or her duties and the need to access certain personal and/or sensitive data, and with security achieved by defining passwords provided to ISTEC Lisboa employees.

## 7.3. Security Copies

In collaboration with the different services, the Office of Information Technology and Systems, and following the RGPG and ISTEC Lisbon's Privacy Policy, must create regular and encrypted mechanisms for these copies and files whose free access can only be given to the institution's data protection officer.

General information:

a. Collaborate with other services to conduct data protection impact assessments whenever necessary, especially in services and projects involving the processing of sensitive or large-scale personal data, identifying and mitigating risks related to privacy and data security.

b. Implement appropriate measures and techniques to ensure the security of personal data under the responsibility of the IT and systems office, including implementation of access controls, data encryption, security monitoring, regular backups, and security incident response plans.

c. Policies and procedures should be established to appropriately manage access to systems and personal data, ensuring that only authorized persons have access to data necessary to perform their duties.

d. Incorporate privacy principles from the beginning of the development and implementation of systems and software. Consider technical measures that ensure the protection of personal data, such as data minimization, anonymization, pseudonymization, and the implementation of privacy settings by default.

e. Establish clear personal data retention and disposal policies, ensuring that data is kept only as long as necessary and is appropriately destroyed when no longer needed, following legal and regulatory requirements.

f. A "clean desk and equipment usage policy" should be implemented and enforced, e.g., no personal data should be exposed and conditional access in the workspace.

g. Email address signatures must contain a confidentiality message.

# Security and Privacy Best Practices

Security and privacy are critical concerns in all areas of ISTEC Lisbon. By following the practices outlined in this manual, we can mitigate the risks of security and privacy breaches and comply with legal obligations related to data protection, while also promoting a layered approach to security and privacy, covering both technical measures and behavioural practices. It includes recommendations on adopting robust authentication systems, implementing firewalls and data encryption, performing regular backups, raising employee awareness of phishing and other threats, and guidelines for secure information sharing and compliance with internal security policies.

## 1. Privacy and Personal Data Protection

The General Data Protection Regulation has been published in the Official Journal of the European Union and is applicable as of May 25, 2018.

Regarding the new regulation, it is important to know that:

a. Personal data is all information concerning an identified or identifiable person (name, address, assets, salary, dates, card numbers, phone number, IP, videos, image, race, biometric data, attendance sheets, evaluations, curriculum vitae, etc).

b. There is a Data Protection Officer (DPO) at ISTEC Lisbon, who can be contacted via email address protecao.dados@istec.pt.

c. When sending personal data to others, these should be encrypted or protected with a password (the password should not be sent via email).

d. Great care should be taken when handling documents with critical information, such as medical or minor personal data.

e. Before sending information via e-mail with a promotional nature, such as information on training courses, training offers or other similar information, make sure that the recipient of the message has given his or her consent to the sending of such information. If you do not have their consent, try to obtain it, by e-mail, before sending the information.

f. When destroying or deleting personal data, they must be permanently erased/ destroyed, thus ensuring that they cannot be recovered by third parties.

g. When there is a violation of personal data and personal data violation is considered a security breach that causes, either accidentally or unlawfully, the destruction, loss, alteration, unauthorized disclosure, or access, to personal data should immediately report the security incident through protecao.dados@istec.pt.

h. The DPO has the responsibility and obligation to report to the authorities all leaks or losses of personal data occurring in the organization unless the personal data breach is not likely to result in a risk to the rights and freedoms of natural persons.

# 2. Electronic Mail

Email is the most widely used communication service in organizations, in that sense it is also a source of risk and one of the most used means for spreading malicious programs. Each user is responsible for the use and activities associated with his or her e-mail account. It must be used appropriately and in a way that does not damage the image or operation of ISTEC Lisbon. It is therefore forbidden to use the email service to send offensive or inappropriate information or content. In the same vein, it is also forbidden to use ISTEC Lisbon email to deal with personal matters.

## 2.1. Email account forwarding

Forwarding emails from internal accounts to external accounts is not recommended. Forwarding messages between internal mailboxes is also discouraged and should only happen with the authorization of the email account owners or in special cases (e.g., illness, vacation, among others).

## 2.2. Check Recipients

When sending messages, it is essential to make sure that the recipients you have included are correct, e.g., that they are the ones who should receive and have access to the information you are sending. If necessary, make good use of the "Surreptitious copy" and "Reply all" options.

## 2.3. Attachments to messages

Email is a popular way for malicious software (malware) to spread. It is important to be aware of this fact when you receive e-mail messages that contain attachments or links to download from external websites. As antivirus software is not infallible, the best defence is prudence, and the following actions are advisable:

a. Do not open attachments of unknown origin.

b. Do not open attachments from known addresses that you did not expect to receive.

c. Never open attachments that have executable extensions (.exe, .bat, .com, .dll).

d. Do not open attachments that have more than one extension.

e. In case of doubt, consult the Information Technology and Systems Office for clarification.

### 2.4. Critical and personal information

Critical, confidential, or other information regarding personal/private data should only be sent via e-mail in encrypted formats. The keys/passwords used in these processes should be sent via another means of communication.

### 2.5. Disclaimer

When sending sensitive information (for example: containing personal, private, secret or confidential data), the e-mail message should be accompanied by a warning/disclaimer stating that the information sent is intended solely for the addressee(s), and its distribution is prohibited.

Example "This message contains information classified as confidential or privileged. In case you have inadvertently received it, please contact the sender by email and delete the message as well as all your data."

## 3. Clean Table Policy and Use of Equipment

All members of ISTEC Lisbon's academic community should consider the clean desk policy to ensure that private, secret or confidential information is not disclosed.

Thus, the following actions should be considered:

a. The work desk shall be cleared of any documents or information media, which contain personal data or secret and/or confidential information when left unattended for an extended period, as well as at the end of the workday.

b. All information containing personal, private, secret, and confidential data shall be removed from the desk after use and stored in a secure, access-controlled location.

c. All documents and physical media of information shall be stored in suitable drawers with locks and/or other secure forms of furniture when not in use, especially outside working hours.

d. Computers and mobile devices should be locked whenever the user is away and turned off at the end of the workday.

e. All printouts containing personal, private, secret or confidential information used or processed by support equipment, for example, printers, photocopiers and/or scanners, shall be removed from them immediately after their processing is completed.

f. No restricted access information may be removed from the premises without authorization.

g. Outside ISTEC Lisbon premises, any element of the academic community is responsible for safeguarding the equipment and information entrusted to it.