Security and GDPR

Policy

Edenred Italia Srl

Via GB Pirelli 18
20124 Milano
Italy
☎ +39 (0) 2 26 904 1
+39 (0) 2 21 309 1
https://www.edenred.it/

Company	Function	Scope
Edenred	CISO - Chief of Information Security Office	Accountable
Edenred	DPO - Data Protection Officer	Consulted
Edenred	Privacy Manager	Responsible
Edenred	Head of Corporate Compliance & Legal	Consulted
Edenred	CIO - Head of Information Technology	Informed
Edenred	Head of IT Infrastructure	Consulted
Edenred	IT Security	Responsible

Reviews					
#	Date	Description	Author	Reviewed by	Approved by
1.0	26/03/2017	First draft	IT Security	IT Security	CIO - Head of Information Technology
1.1	13/07/2017	Update of the chapter 16	IT Security	IT Security	CIO - Head of Information Technology
2.0	21/05/2018	Review of the document to integrate improved technical measures for GDPR and change of the logo.	IT Security	IT Security	CIO - Head of Information Technology
2.1	12/11/2018	Change of the document classification to public document	IT Security	IT Security	CIO - Head of Information Technology
2.2	04/09/2019	Review of the document to integrate improved technical measures. Change approver	IT Security	IT Security	CISO - Chief of Information Security Office
3.0	28/05/2021	Change of document template and general review of the contents	IT Security	DPO - Data Protection Officer	CISO - Chief of Information Security Office
3.1	10/01/2023	Update of chapter from 1 to 16	Information Security Consultant	DPO - Data Protection Officer	CIO - Head of Information Technology

Summary

1. Introduction

1.1. Aim of the document

This document describes all information security and privacy measures that Edenred Italia S.r.l. adopts, relevant for complying both with the GDPR, the standard ISO/IEC 27001 and the standard ISO/IEC 27701.

In round brackets it is specified whether an ISO/IEC 27001 or ISO/IEC 27701 control is technical or organizational

1.2. Terms and definitions

term	definition
GDPR	General Data Protection Regulation EU 2016/679
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISO/IEC 27001	It is an information security standard, part of the ISO/IEC 27000 family of standards, of which the latest version was released in 2013. It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee.
ISO/IEC 27701	**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**
PII	Personally Identifiable Information; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

2. Information Security and Privacy Policies

This chapter, traceable to the standard ISO/IEC 27001 control A.5 and to the standard ISO/IEC 27701 control 6.2, describes how Edenred Italia S.r.l. manages its own information security and privacy higher-level policies.

2.1. Management direction for information security and privacy (organizational)

Edenred Italia S.r.l. has defined, published and provided a set of information security and privacy policies covering the most relevant aspects of the topic, constantly keeping every document up-to-date.

This paragraph is linked to the objective control A.5.1.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.2.1.1 of the standard ISO/IEC 27701.

2.2. Risk management for information security and privacy (organizational)

Edenred Italia S.r.l. has defined a risk management process to handle information security and data protection. This process is based on MAGERIT Methodology and PILAR Software Platform.

This paragraph is linked to the objective control A.5.1.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.2.1.2 of the standard ISO/IEC 27701.

3. Organization of information security and privacy

This chapter, traceable to the standard ISO/IEC 27001 control A.6 and to the standard ISO/IEC 27701 control 6.3, describes how Edenred Italia S.r.l. has organized its own roles and responsibilities for information security and data protection management.

3.1. Internal organization (organizational)

Relevant roles for information security and data protection management have been defined and any responsibilities related to each of them have been identified. The interested personnel have then received an official letter of appointment on those bases.

This paragraph is linked to the objective controls A.6.1.1 and 6.1.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.3.1.1 and 6.3.1.2 of the standard ISO/IEC 27701.

3.2. Contact with authorities (organizational)

Edenred Italia S.r.l. has defined the processes that manage the contact with authorities, describing the workflows and identifying the ownership of the Company departments for each step of them.

This paragraph is linked to the objective control A.6.1.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.3.1.3 of the standard ISO/IEC 27701.

3.3. Contact with special interest group (organizational)

Edenred Italia S.r.l. has identified the special interest group related to the Information Security and Privacy Management System from which the Company collects relevant updates on this topic.

This paragraph is linked to the objective control A.6.1.4 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.3.1.4 of the standard ISO/IEC 27701.

3.4. Information security and privacy in project management (organizational)

Security is a relevant issue in any project carried out by Edenred Italia S.r.l. Therefore, all the projects include security topics.

This paragraph is linked to the objective control A.6.1.5 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.3.1.5 of the standard ISO/IEC 27701.

3.5. Mobile devices and telework (organizational)

Out of office personnel can use an authorized internet connection to access via secure VPN to the Edenred network.

This paragraph is linked to the objective control A.6.2.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.3.2.1 of the standard ISO/IEC 27701.

3.6. Teleworking (organizational)

Edenred Italia S.r.l. envisages teleworking and smart working. The company adopts adequate security measures to protect its own devices and assets; furthermore, all employees and collaborators are trained to protect Company information and devices during teleworiking or smart working.

This paragraph is linked to the objective control A.6.2.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.3.2.2 of the standard ISO/IEC 27701.

4. Human resource security

This chapter, traceable to the standard ISO/IEC 27001 control A.7 and to the standard ISO/IEC 27701 control 6.4, describes how Edenred Italia S.r.l. implements information security and privacy with regards to its personnel.

4.1. Prior to employment (organizational)

Additionally to competence screenings related with the hiring position, criminal records for every potential new employee are requested and verified before the contract begins.

A formal approval of the Code of Ethics is also required.

This paragraph is linked to the objective controls A.7.1.1 and A.7.1.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.4.1.1 and 6.4.1.2 of the standard ISO/IEC 27701.

4.2. During employment (organizational)

Each new employee must complete a self-training for information security and data protection with an annual renewal. After the training a test is performed to validate his understanding. If the score is not sufficient the training must be repeated.

A compendium is provided to all employees with information security and data protection information.

If employees does not follow the Company rules on information security and data protection, they undergo a disciplinary process.

This paragraph is linked to the objective controls A.7.2.1, A.7.2.2 and A.7.2.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.4.2.1, 6.4.2.2 and 6.4.2.3 of the standard ISO/IEC 27701.

4.3. Termination and change of employment (organizational)

A formal verification of all assets and permissions assigned to a person changing or terminating its position is performed, based on a dedicated checklist.

This paragraph is linked to the objective control A.7.3.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.4.3.1 of the standard ISO/IEC 27701.

5. Asset Management

This chapter, traceable to the standard ISO/IEC 27001 control A.8 and to the standard ISO/IEC 27701 control 6.5, describes how Edenred Italia S.r.l. implements information security and privacy through its own asset management process.

5.1. Responsibility for assets (organizational)

Asset inventories are kept up-to-date in order to track all Edenred Italia S.r.l. assets, including hardware and software, and their assignee. In particular, all workstations are assigned and withdrawn using tickets required by the employee's manager.

Asset users are fully instructed on the acceptable use of their assigned assets before having them at their disposal.

This paragraph is linked to the objective controls A.8.1.1, A.8.1.2, A.8.1.3 and A.8.1.4 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.5.1.1, 6.5.1.2, 6.5.1.3 and 6.5.1.4 of the standard ISO/IEC 27701.

5.2. Information classification (organizational)

Storing data on local workstations is prohibited by policy. All data have to be stored in the secured DMS or other collaboration tools approved by the top management and abide to the information classification policy guidelines, which regulate their expected handling and also drive their labelling. By default, each workstation's hard disk is encrypted.

This paragraph is linked to the objective controls A.8.2.1, A.8.2.2 and A.8.2.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.5.2.1, 6.5.2.2 and 6.5.2.3 of the standard ISO/IEC 27701.

5.3. Media handling (organizational)

Edenred Italia S.r.l. media are subject to specific handling rules related to the classification level of stored information. Those rules cover authorized copy, electronic and physical transmission, printing and secure deletion operations performed on media.

The use of removable media is allowed. However, users must follow security rules and best practices to protect the information stored in. Furthermore, sensitive data cannot be stored in removable media.

This paragraph is linked to the objective controls A.8.3.1, A.8.3.2 and A.8.3.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.5.3.1, 6.5.3.2 and 6.5.3.3 of the standard ISO/IEC 27701.

6. Access control

This chapter, traceable to the standard ISO/IEC 27001 control A.9 and to the standard ISO/IEC 27701 control 6.6, describes how Edenred Italia S.r.l. manages accesses to its own information and related systems.

6.1. Business requirements of access control (organizational)

An overall access management policy is implemented in Edenred Italia S.r.l. regulating access profiles for all information systems and applications.

Each workstation is configured by ICT team, to access at the local network area, with the maximum restriction. Any grant to access to servers or internet has to be approved by the competent administrator, using the dedicated ticketing system. It is never permitted to open a ticket to oneself.

To access Internet the requestor has to compile a module with the signature of the area manager. There are different levels of internet access accordingly to the employee's job profile needs.

Only workstations or mobile devices configured and secured by ICT team can access to the network.

Internet browsing is monitored in compliance with local laws for workers control and web filtering is active.

All Administrator have personal credentials and their sharing is strictly prohibited.

This paragraph is linked to the objective controls A.9.1.1 and 9.1.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.6.1.1 and 6.6.1.2 of the standard ISO/IEC 27701.

6.2. User access management (technical)

Each user is associated with a unique userID and their initial password is supplied in a confidential way.

Each request to create, delete or update an employee's account has to be tracked with the ticketing system starting from the request by the responsible person.

Profiles access rules and grants are established following the least privilege and the need to know principles and are reviewed at least yearly, both at an operating system level and at an application level. All main applications are linked with the operating system access management system.

This paragraph is linked to the objective controls A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5 and A.9.2.6 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.6.2.1, 6.6.2.2, 6.6.2.3, 6.6.2.4, 6.6.2.5 and 6.6.2.6 of the standard ISO/IEC 27701.

6.3. User responsibilities (organizational)

Edenred Italia S.r.l. users are made aware of the intended correct use of their assigned credentials, both on the enterprise information systems and on other ones.

This paragraph is linked to the objective control A.9.3.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.6.3.1 of the standard ISO/IEC 27701.

6.4. System and application access control (technical)

Secure credentials management rules are established and enforced through the operating system access management system, including:

- expiration set to 90 days;
- minimum length set to 10 characters;
- initial password is required to be changed at first logon;
- complexity requirements are active;
- password history (a new password must be different to the previous 24 passwords);
- user right reviewed at least twice per year.

Password resets are securely performed, applying measures to recognize the requestor and thus avoiding user masquerading.

Multi-factor authentication (MFA) is implemented to ensure a higher level of security. Users access will be granted only after having inserted a validation token. Users can access to applications only if they have a specific authorization.

This paragraph is linked to the objective controls A.9.4.1, A.9.4.2 and A.9.4.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.6.4.1, 6.6.4.2 and 6.6.4.3 of the standard ISO/IEC 27701.

6.5. Use of privileged utility programs (technical)

Edenred Italia S.r.l. does not allow the use of privileged utility programs, in order to avoid the decrease of efficiency of development activities.

This paragraph is linked to the objective control A.9.4.4 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.6.4.4 of the standard ISO/IEC 27701.

6.6. Access control to program source code (organizational)

The systems to access to Edenred Italia S.r.l. source code collect all the logs and the security criteria to access to the source code are in line with the best practices.

This paragraph is linked to the objective control A.9.4.5 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.6.4.5 of the standard ISO/IEC 27701.

7. Cryptography

This chapter, traceable to the standard ISO/IEC 27001 control A.10 and to the standard ISO/IEC 27701 control 6.7, describes how Edenred Italia S.r.l. uses cryptography to protect relevant information.

7.1. Cryptographic control (technical)

Encryption is used by Edenred Italia S.r.l. to protect all confidential data in transit over untrusted telecommunications network (like the Internet). State of the art certificates, protocols, and encryption ciphers are adopted in those cases.

Edenred Italia S.r.l. does not manage encryption keys, since the Company does not adopt solutions that need key management.

This paragraph is linked to the objective controls A.10.1.1 and A.10.1.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.7.1.1 and 6.7.1.2 of the standard ISO/IEC 27701.

8. Physical and environmental security

This chapter, traceable to the standard ISO/IEC 27001 control A.11 and to the standard ISO/IEC 27701 control 6.8, describes how Edenred Italia S.r.l. manages its physical security in order to protect the security of information.

8.1. Secure areas (technical)

Edenred Italia S.r.l. main building access is permitted only through turnstiles with badge. Guests can enter without a badge after registration and must be always escorted by an internal employee.

Each plan is accessible only with an authorized badge. All maintenance personnel must be registered and a personal badge is assigned to them.

A guarded reception is present at the entrance.

Server rooms are accessible through a badge with specific permissions. Each permission must be required by managers and duly registered.

The access to the room is recorded by a surveillance camera monitoring 24H/24H. Registrations are handled and destroyed within the terms defined by the law.

This paragraph is linked to the objective controls A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5 and A.11.1.6 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.8.1.1, 6.8.1.2, 6.8.1.3, 6.8.1.4, 6.8.1.5 and 6.8.1.6 of the standard ISO/IEC 27701.

8.2. Equipment (technical)

All Edenred Italia S.r.l. servers and relevant telecommunications systems are located either within the aforementioned server room or at a trusted Group's service provider's premises and can be moved from there only with previous authorization. Their maintenance, as the correct management of cabling is ensured by qualified outsourcers.

Screen blocking is set after 15 minutes of inactivity.

This paragraph is linked to the objective controls A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 and A.11.2.9 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.8.2.1, 6.8.2.2, 6.8.2.3, 6.8.2.4, 6.8.2.5, 6.8.2.6, 6.8.2.7 6.8.2.8 and 6.8.2.9 of the standard ISO/IEC 27701.

9. Operations security

This chapter, traceable to the standard ISO/IEC 27001 control A.12 and to the standard ISO/IEC 27701 control 6.9, describes how Edenred Italia S.r.l. manages its own IT operations ensuring the security of processed information.

9.1. Operational procedures and responsibilities (organizational)

Edenred Italia S.r.l. has developed a set of documented procedures to regulate all key ICT activities which have a relationship with information security and privacy information management, among which backup, system configuration, audit log management and monitoring. Those procedures are made promptly available to the personnel in charge of their implementations.

This paragraph is linked to the objective control A.12.1.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.9.1.1 of the standard ISO/IEC 27701.

9.2. Change Management

Edenred Italia S.r.l. adopts a change management process and documented procedure for manage change request. Every change has been identified, recorded, planned, tested (including fallback procedures), assessed from the perspective of impacts on service and security, approved with a formal process, communicated and managed in emergency mode, if it needs, to solve an incident.

This paragraph is linked to the objective control A.12.1.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.9.1.2 of the standard ISO/IEC 27701.

9.3. Capacity Management

Edenred Italia S.r.l. uses a capacity management process and procedure periodically for optimization through fine tuning of application, system, database and all in scope system and recovery ICT resource trough decommissioning and erasing.

This paragraph is linked to the objective control A.12.1.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.9.1.3 of the standard ISO/IEC 27701.

9.4. Separation of development, testing and operational environments

Edenred Italia S.r.l. uses a separate environment for development, testing and production.

Only infrastructure services are common and “security hardening” for use.

This paragraph is linked to the objective control A.12.1.4 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.9.1.4 of the standard ISO/IEC 27701.

9.5. Protection from malware (technical)

All workstations and malware-prone servers are equipped with an antivirus that cannot be disabled or changed by the end-user. The antivirus’ update is centrally executed with adequate frequency.

This paragraph is linked to the objective control A.12.2.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.9.2.1 of the standard ISO/IEC 27701.

9.6. Backup (technical)

There are two different types of backups: complete backup, performed weekly, and incremental backup performed daily. Every weekend all backups are cloned and sent in a data bank with retention for 4 weeks.

Every month an integrity test of the backups with a restore test is performed.

Every day the backup system sends an email with a report of all performed backup. The ICT team monitors these mails and promptly manages errors.

This paragraph is linked to the objective control A.12.3.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.9.3.1 of the standard ISO/IEC 27701.

9.7. Logging and monitoring (technical)

A dedicated tool constantly and continuously monitors the logical infrastructures and systems status. The tool shows the current status using a “traffic light” representation, with different colors to represent different statuses. ICT team monitors constantly this tool and during not working hours an email is sent at ICT teams to manage any arising problem remotely.

All login and logout are recorded and the related evidence are stored for at least 6 months and periodically analyzed.

The clocks of all relevant information processing system of Edenred Italia S.r.l. are synchronized with a single external reference time source.

This paragraph is linked to the objective controls A.12.4.1, A.12.4.2, A.12.4.3 and 12.4.4 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.9.4.1, 6.9.4.2, 6.9.4.3 and 6.9.4.4 of the standard ISO/IEC 27701.

9.8. Control of operational software (technical)

A centralized software for detecting and applying vendor patches is used for both client and server environments. Application environments are updated periodically in order to keep them aligned with security patches.

This paragraph is linked to the objective control A.12.5.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.9.6.1 of the standard ISO/IEC 27701.

9.9. Technical vulnerability management (technical)

Technical vulnerabilities are collected both through the aforementioned software for the control of operational software and through the performance of periodical vulnerability assessment activities. Users are also not administrators of their workstations, so they are not authorized to install autonomously any software on them.

This paragraph is linked to the objective control A.12.6.1 and A.12.6.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.9.6.1 and 6.9.6.2 of the standard ISO/IEC 27701.

9.10. Information systems audit considerations (technical)

There are no relevant information system audit features to be secured on Edenred Italia S.r.l. systems.

This paragraph is linked to the objective control A.12.7.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.9.7.1 of the standard ISO/IEC 27701.

10. Communications security

This chapter, traceable to the standard ISO/IEC 27001 control A.13 and to the standard ISO/IEC 27701 control 6.10, describes how Edenred Italia S.r.l. manages its networks ensuring the security of transmitted information.

10.1. Network security management (technical)

Edenred Italia S.r.l. internal network is configured in separate areas segregated via duly configured firewalls, which are maintained by a third-party subject independent from server administrators. Its main components have been designed and configured to ensure high availability levels.

This paragraph is linked to the objective controls A.13.1.1, A.13.1.2 and A.13.1.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.10.1.1, 6.10.1.2 and 6.10.1.3 of the standard ISO/IEC 27701.

10.2. Information transfer (technical)

When necessary Edenred Italia S.r.l. uses external partner to dispatch business services. All connections with external partners are transmitted on a dedicated VPN and data transfer is executed using SFTP with specific access login.

Company documents can be transferred by email, only if the enclosed documents are encrypted using the AES-256 protocol and the password to open them is communicated through alternative channel (e.g. SMS).

This paragraph is linked to the objective control A.13.2.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.10.2.2 of the standard ISO/IEC 27701.

10.3. Electronic messaging (technical)

Edenred Italia S.r.l. protects email messaging from unauthorized access, modification, denial of service, spam, phishing and any other attempted fraud. Edenred Italia S.r.l. account are protected, monitored and the security solutions used are updated periodically. Simulated phishing campaigns are carried out periodically to test the efficiency of the systems and the effectiveness of training and awareness-raising actions.

This paragraph is linked to the objective control A.13.2.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.10.2.3 of the standard ISO/IEC 27701.

10.4. Confidentiality or non-disclosure agreements (organizational)

Edenred Italia S.r.l. requires the signature of non-disclosure agreements before transferring Company information, in order to protect confidentiality.

This paragraph is linked to the objective control A.13.2.4 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.10.2.4 of the standard ISO/IEC 27701.

11. System acquisition, development and maintenance

This chapter, traceable to the standard ISO/IEC 27001 control A.14 and to the standard ISO/IEC 27701 control 6.11, describes how Edenred Italia S.r.l. securely maintains and evolves its information systems and software.

11.1. Security requirements of information system (technical)

Edenred Italia S.r.l. has adopted several best practices for software development, including information security among formalized requirements. Development tools usage in compliance to those best practices has been defined and proceduralized. All relevant development personal is periodically trained on secure coding.

This paragraph is linked to the objective controls A.14.1.1, A.14.1.2 and A.14.1.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.11.1.1, 6.11.1.2 and 6.11.1.3 of the standard ISO/IEC 27701.

11.2. Security in development and support process (technical)

Secure System Development Life Cycle Policy and software development project guidelines are used to govern development and support activities within Edenred Italia S.r.l.

Software changes to Edenred Italia S.r.l. software are regulated through formal change request processes, where approval is a separate responsibility from development. Formal acceptance tests are conducted and registered before a change is successfully closed. All software changes are tracked by centralized versioning platform and software code are reviewed by centralized security code analyzer for identification and fix bug or issue and intercept training opportunity.

Vendor-acquired software packages modification is not performed and generally discouraged.

This paragraph is linked to the objective controls A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8 and A.14.2.9 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.11.2.1, 6.11.2.3, 6.11.2.3, 6.11.2.5, 6.11.2.6, 6.11.2.7, 6.11.2.8 and 6.11.2.9 of the standard ISO/IEC 27701.

11.3. Test data (technical)

Edenred Italia S.r.l. adopts procedures and techniques for the transformation of production data required to be used on test environments, in order to reduce the sensitiveness of personal data used for software development purposes.

Additionally, test environments are physically and/or logically separated from production environments to allow the presence of more restricted accesses on the latter one.

This paragraph is linked to the objective control A.14.3.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.11.3.1 of the standard ISO/IEC 27701.

12. Supplier relationships

This chapter, traceable to the standard ISO/IEC 27001 control A.15 and to the standard ISO/IEC 27701 control 6.12, describes how Edenred Italia S.r.l. manages information security and privacy with its own suppliers.

12.1. Information security and privacy in supplier relationships (organizational)

Standardized non-disclosure agreements with relevant suppliers are negotiated and included within their contracts. Additional information security and privacy-based considerations or service levels are applied on a case by case policy depending on the supplied services/goods, Cloud Service Provider included. Dedicated DPAs are also established depending on the personal data protection role of the supplier.

This paragraph is linked to the objective controls A.15.1.1, A.15.1.2 and A.15.1.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.12.1.1, 6.12.1.2 and 6.12.1.3 of the standard ISO/IEC 27701.

12.2. Supplier service delivery management (organizational)

Supplier's services of high relevance for Edenred Italia S.r.l. are kept under periodical monitoring against the negotiated SLAs, enabling to request improvements to their services' quality where and when needed.

This paragraph is linked to the objective controls A.15.2.1 and A.15.2.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.12.2.1 and 6.12.2.3 of the standard ISO/IEC 27701.

13. Information security and privacy incident management

This chapter, traceable to the standard ISO/IEC 27001 control A.16 and to the standard ISO/IEC 27701 control 6.13, describes how Edenred Italia S.r.l. manages information security incidents.

13.1. Management of information security and privacy incidents and improvements (organizational)

ICT incident monitoring is continuously performed within Edenred Italia S.r.l. Whenever a suspect potential incident is detected, a ticket is registered and a pre-defined series of actions is performed to analyze it and subsequently address it, minimizing the impact to the organization's services and information. Dedicated data breach management procedures are also established and followed.

Incident resolution activities are periodically reviewed to improve the effectiveness of the pre-defined actions to be performed.

This paragraph is linked to the objective controls A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6 and A.16.1.7 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.13.1.1, 6.13.1.2, 6.13.1.3, 6.13.1.4, 6.13.1.5, 6.13.1.6 and 6.13.1.7 of the standard ISO/IEC 27701.

14. Information security and privacy aspects of business continuity management

This chapter, traceable to the standard ISO/IEC 27001 control A.17 and to the standard ISO/IEC 27701 control 6.14, describes how Edenred Italia S.r.l. manages information security in situations where the business continuity is at stake.

14.1. Information security and privacy continuity (organizational)

All continuity procedures have been developed in order to maintain the same information security level existing before their activation.

This paragraph is linked to the objective controls A.17.1.1, A.17.1.2 and A.17.1.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.14.1.1, 6.14.1.2 and 6.14.1.3 of the standard ISO/IEC 27701.

14.2. Redundancies (technical)

A business continuity plan is present to prevent events that could stop the Edenred Italia S.r.l. operations. The plan focuses on:

- Energy blackout: both short and long time.
- Inaccessible building.
- Air conditioning failure in the server room.
- Connectivity failures.
- Datacenter related failures.

The plan identifies different cases on the basis of the expected unavailability time.

This paragraph is linked to the objective control A.17.2.1 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.14.2.1 of the standard ISO/IEC 27701.

15. Compliance

This chapter, traceable to the standard ISO/IEC 27001 control A.18 and to the standard ISO/IEC 27701 control 6.15, describes how Edenred Italia S.r.l. manages compliance to the elements specifying effective information security and privacy requirements.

15.1. Compliance with legal and contractual requirements (organizational)

Edenred Italia S.r.l. annually reviews its information security and data protection constraints within the scope of its own ISO/IEC 27001, ISO/IEC 27701 certifications and the legal and technical requirements of the GDPR, considering applicable legal and contractual requirements.

Edenred Italia S.r.l. also ensures the intellectual property rights and the protection of records, in compliance with the effective legislation.

There are not national or industry regulation on cryptographic controls.

This paragraph is linked to the objective controls A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4 and A.18.1.5 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.15.1.1, 6.15.1.2, 6.15.1.3, 6.15.1.4 and 6.15.1.5 of the standard ISO/IEC 27701.

15.2. Information security and privacy reviews (organizational)

Edenred Italia S.r.l., since it is an ISO/IEC 27001 and ISO/IEC 27701 certified company, develops and carries out annually a program of both internal and external audit on those schemes, ensuring a constant third-party double control on information security and privacy.

This paragraph is linked to the objective controls A.18.2.1 and A.18.2.2 of the standard ISO/IEC 27001.

This paragraph is linked to the objective controls 6.15.2.1 and 6.15.2.2 of the standard ISO/IEC 27701.

15.3. Technical security reviews (organizational)

Edenred Italia S.r.l. periodically relies on specialized companies for an independent assessment of the security of its systems through vulnerability assessments and penetration tests. For company policy and agreement with cloud service providers these reports are not disclosed but available for internal audit and certification body activities.

This paragraph is linked to the objective control A.18.2.3 of the standard ISO/IEC 27001.

This paragraph is linked to the objective control 6.15.2.3 of the standard ISO/IEC 27701.

16. Data Protection

This chapter, traceable to the standard ISO/IEC 29100 Annex A, describes how Edenred Italia S.r.l. manages personal data protection related topics extending beyond information security.

16.1. General policies for the use and protection of PII (organizational)

Edenred Italia S.r.l. has developed a privacy policy following the guidelines coming from applicable best practices that meet GDPR requirements.

16.2. Consent and choice (organizational)

All data processing consents proposed by Edenred Italia S.r.l. have been reviewed in light of GDPR, allowing the data subject to freely perform his/her choices for separate purposes where applicable. Data subjects are informed whether their consent is required to proceed with processing activities within all data protection notices, which contents are in line with GDPR requirements.

This paragraph is linked to the Privacy Principle n.1 of ISO/IEC 29100.

16.3. Purpose legitimacy and specification (organizational)

Edenred Italia S.r.l. has reviewed all bases for all performed personal data processing in order to have them aligned to GDPR related requirements. Gathered bases are inventoried within the records of processing activities.

Data protection notices provide accurate information about the purpose of collection and processing, in line with the Group's guidelines.

This paragraph is linked to the Privacy Principle n.2 of ISO/IEC 29100

16.4. Collection limitation (organizational)

Collected personal data are minimized within all personal data processing activities. The collection of personal data belonging to special categories is always avoided wherever feasible.

This paragraph is linked to the Privacy Principle n.3 of ISO/IEC 29100

16.5. Data minimization (organizational)

In addition to limiting the collection of personal data, Edenred Italia S.r.l. minimizes the amount of personal data being processed for fulfilling each purpose. This includes applying additional restrictions to data accesses permissions and the implementation of other information security and Privacy Enhancing Techniques.

Personal data being communicated to third parties, where applicable, are also being analyzed for minimization opportunities.

This paragraph is linked to the Privacy Principle n.4 of ISO/IEC 29100

16.6. Use, retention and disclosure limitation (organizational)

Edenred Italia S.r.l. manages the business logic with which personal data are managed throughout its applications in order to enable a distinction between the different purposes for personal data processing and to allow an automatic management of their retention and subsequent secure deletion / anonymization when this expires.

Personal data retention time is set accordingly to contractual and legal obligations and for a proportionate amount of time.

This paragraph is linked to the Privacy Principle n.5 of ISO/IEC 29100

16.7. Accuracy and quality (technical)

Edenred Italia S.r.l. collects personal data with specific attention to their accuracy and quality also performing input validations checks and ultimately allowing data subject to promptly update them in case any need arises. Direct interaction with the data subject is always pursued in order to minimize errors caused by any relaying process.

This paragraph is linked to the Privacy Principle n.6 of ISO/IEC 29100

16.8. Openness, transparency and notice (organizational)

Data protection notices are written in order to maximize their clarity to every data subject and providing clear information on Edenred Italia S.r.l. procedures, processes and means used for personal data processing.

Edenred Italia S.r.l. is also versioning its data protection notices to enable a reconstruction of what the data subject was presented to when processing activities commenced.

This paragraph is linked to the Privacy Principle n.7 of ISO/IEC 29100

16.9. PII principal participation and access (organizational)

Edenred Italia S.r.l. has developed processes allowing the timely exercise of data subject's rights in covering all rights included in GDPR.

Those processes include complaints and data breach notification management. This paragraph is linked to the Privacy Principle n.8 of ISO/IEC 29100.

16.10. Accountability (organizational)

Edenred Italia S.r.l. has adopted an organizational structure involving a formally designated Data Protection Officer.

Procedures to evaluate the need of performing Data Protection Impact Assessment activities and to guide their execution in line with applicable best practices and group's indications are present. Supplier management is reinforced with assurance procedures aiming to require sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the GDPR requirements and ensure the protection of the rights of the data subject.

Operations executed on personal data are subject to a closer and more structured monitoring, including the secure storage of audit logs, especially when performed by system administrator personnel.

A training program comprising those procedures and the requirements present in GDPR is transversally planned for all Edenred Italia S.r.l. personnel.

This paragraph is linked to the Privacy Principle n.9 of ISO/IEC 29100

16.11. Information Security (organizational)

Edenred Italia S.r.l. protects PII under its own authority, to guarantee integrity, confidentiality and availability, and protects it from risks such as unauthorized access, use, destruction, modification and disclosure through specific controls based on legal requirements, risk assessments and security standards.

The level of controls is directly proportional to the sensitivity of the PII, the likelihood and severity of the consequences of its disclosure, and the context in which it is stored.

These controls are designed according to the principle of 'least privilege' and are subject to a periodic review, reassessment, and update process, following vulnerability assessment, to ensure proper risk management.

This paragraph is linked to the Privacy Principles n.10 of ISO/IEC 29100

16.12. Privacy compliance (organizational)

Edenred Italia S.r.l. launched a dedicated program both at a national and at international level in 2017 aiming to review the posture of the enterprise towards the requirements of the new Regulation and to improve its personal data processing activities, which has been followed by an additional Group level program to enhance data protection practices beyond GDPR requirements in 2020.

This paragraph is linked to the Privacy Principle n.11 of ISO/IEC 29100