	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
Status (first draft, reviewed, approved)	approved	



Security and GDPR

Information security and data protection measures

Public document


Edenred Italia Srl Direzione DSI

Via GB Pirelli 18
20124 Milano
Italy

☎ +39 (0) 2 26 904 1

📠 +39 (0) 2 21 309 1


<http://www.edenred.com/>

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

Company	Recipients	#	Approves	Comments	Informed
Edenred	Antonio Bacci	1		✓	✓
Edenred	Claudio D'Angelo	2		✓	✓
Edenred	Paolo Musazzi	3	✓	✓	✓
Edenred	Elena Bianco	4		✓	✓
Bl4ckswan Srl	Pasquale Scalea	5		✓	✓


Reviews					
#	Date	Description	Author	Reviewed by	Approvedby
1.0	26/03/2018	First draft	CDA	CDA	AB
1.1	13/07/2017	Update of the data protection chapter	CDA	CDA	AB
2.0	21/05/2018	Review of the document to integrate improved technical measures for GDPR and change of the logo.	CDA	CDA	AB
2.1	12/11/2018	Changed the document classification to public document	CDA	CDA	AB
2.2	04/09/2019	Review of the document to integrate improved technical measures. Change approver	PS	CDA	PM

Confidentiality
The present document contains proprietary information that must be kept confidential. The document and all of its contents are property of Edenred Italia S.r.l. and cannot be spread, sent, copied, showed or otherwise distributed without an explicit authorization from Edenred Italia S.r.l.


	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

Summary

1. Overview	5
1.1. Glossary	5
2. Information security policies	5
2.1. Management direction for information security (organizational)	5
2.2. Risk Management for information security	5
3. Organization of information security	5
3.1. Internal organization	6
3.2. Mobile devices and telework	6
4. Human resource security	6
4.1. Prior to employment (organizational)	6
4.2. During employment (organizational)	6
4.3. Termination and change of employment (organizational)	6
5. Asset management	6
5.1. Responsibility for assets (organizational)	6
5.2. Information classification (organizational)	7
5.3. Media handling (organizational)	7
5.4. Removable Media (organizational)	7
6. Access control	7
6.1. Business requirements of access control (organizational)	7
6.2. User access management (technical)	7
6.3. User responsibilities (organizational)	8
6.4. System and application access control (technical)	8
7. Cryptography	8
7.1. Cryptographic controls (technical)	8
8. Physical and environmental security	8
8.1. Secure areas (technical)	8
8.2. Equipment (technical)	9
9. Operations security	9
9.1. Operational procedures and responsibilities (organizational)	9
9.2. Change Management	9
9.3. Capacity Management	9
9.4. Separation of development, testing and operational environment	9
9.5. Protection from malware (technical)	10
9.6. Backup (technical)	10
9.7. Logging and monitoring (technical)	10
9.8. Control of operational software (technical)	10
9.9. Technical vulnerability management (technical)	10

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
Status (first draft, reviewed, approved)	approved	

9.10.	Information systems audit considerations (technical)	10
9.11.	Clock Synchronization	10
10.	Communications security	11
10.1.	Network security management (technical)	11
10.2.	Information transfer (technical)	11
10.3.	Electronic messaging	11
11.	System acquisition, development and maintenance.....	11
11.1.	Security requirements of information systems (technical)	11
11.2.	Security in development and support processes (technical)	11
11.3.	Test data (technical)	12
12.	Supplier relationships	12
12.1.	Information security in supplier relationships (organizational)	12
12.2.	Supplier service delivery management (organizational)	12
13.	Information security incident management	12
13.1.	Management of information security incidents and improvements (organizational).....	12
14.	Information security aspects of business continuity management	12
14.1.	Information security continuity (organizational)	13
14.2.	Redundancies (technical)	13
15.	Compliance	13
15.1.	Compliance with legal and contractual requirements (organizational).....	13
15.2.	Information security reviews (organizational)	13
15.3.	Technical security reviews (organizational).....	13
16.	Data protection	13
16.1.	General policies for the use and protection of PII (organizational)	14
16.2.	Consent and choice (organizational).....	14
16.3.	Purpose legitimacy and specification (organizational).....	14
16.4.	Collection limitation (organizational)	14
16.5.	Data minimization (organizational).....	14
16.6.	Use, retention and disclosure limitation (organizational)	14
16.7.	Accuracy and quality (technical)	15
16.8.	Openness, transparency and notice (organizational)	15
16.9.	PII principal participation and access (organizational)	15
16.10.	Accountability (organizational)	15
16.11.	Privacy compliance (organizational)	15

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

1. Overview

This document describes all information security measures that Edenred Italia adopts relevant for complying both GDPR and ISO/IEC 27001.

In square parenthesis it is supplied the documents' location in the ISO/IEC 27001 repository.

1.1. Glossary

Acronym	Description
GDPR	General Data Protection Regulation UE 2016/679
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISO/IEC27001	It's an information security standard, part of the ISO/IEC 27000 family of standards , of which the last version was published 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 JTC 1/SC 27 .



2. Information security policies

This chapter, traceable to ISO/IEC 27001 A.5, describes how Edenred Italia manages its information security higher-level policies.

2.1. Management direction for information security (organizational)


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

2.2. Risk Management for information security

Edenred Italia has defined a risk management process for manage information security, based on Magerit Methodology and Pilar Software Platform

3. Organization of information security

This chapter, traceable to ISO/IEC 27001 A.6, describes how Edenred Italia has organized its roles and responsibilities for information security management.

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

3.1. Internal organization

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

3.2. Mobile devices and telework

Out of office personnel can use an authorized internet connection to access via secure VPN to the Edenred network. No BYOD device is permitted for access to Edenred network or manage company data.

4. Human resource security

This chapter, traceable to ISO/IEC 27001 A.7, describes how Edenred Italia implements information security with regards to its personnel.

4.1. Prior to employment (organizational)

Additionally to competence verifications related with the hiring position, criminal records for every potential new employee are requested and verified before the contract comes in place.

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

4.2. During employment (organizational)

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

A compendium is supplied to all employees with information security and privacy information.

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.

5. Asset management

This chapter, traceable to ISO/IEC 27001 A.8, describes how Edenred Italia implements information security through its asset management process.

5.1. Responsibility for assets (organizational)

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

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

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

5.2. Information classification (organizational)

Saving data on local workstations is prohibited by policy. All data have to be saved in the secured DMS and abide to the information classification policy guidelines, which regulate their expected handling and also drive their labelling. By default the workstation hard disk is encrypted

5.3. Media handling (organizational)

Edenred Italia 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.

5.4. Removable Media (organizational)

Edenred Italia accept use of removable media (USB,CD,etc) only if it is not possible to use the appropriate company data exchange systems and only by adopting the encryption of the device (for example bitlocker) or the contents (for example encrypted zip file). The decryption key must be communicated and stored in a secure manner.

6. Access control

This chapter, traceable to ISO/IEC 27001 A.9, describes how Edenred Italia manages accesses to its information and related systems.

6.1. Business requirements of access control (organizational)

An overall access management policy is implemented in Edenred Italia 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 ticket 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 three levels of internet access: base, advanced and streaming.

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 a personal credential and its sharing is prohibited.

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.

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

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.

6.3. User responsibilities (organizational)

Edenred Italia users are sensibilized on what is the intended correct use of their assigned credentials, both on the enterprise information systems and on other ones.

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 8 characters;
- initial password is required to be changed at first logon;
- complexity requirements are active;
- history.
- User right reviewed at least semi-annually

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

7. Cryptography

This chapter, traceable to ISO/IEC 27001 A.10, describes how Edenred Italia uses cryptography to protect relevant information.

7.1. Cryptographic controls (technical)

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


8. Physical and environmental security

This chapter, traceable to ISO/IEC 27001 A.11, describes how Edenred Italia manages its physical security in order to protect the security of information.

8.1. Secure areas (technical)

Edenred Italia main building access is permitted only through turnstiles with badge. Guests can enter without a badge after registration but always with escort.

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

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
Status (first draft, reviewed, approved)	approved	

A reception with an armed guard is present at the entrance.

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

8.2. Equipment (technical)

All Edenred Italia servers and relevant telecommunications systems are located within the aforementioned server room 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.

9. Operations security

This chapter, traceable to ISO/IEC 27001 A.12, describes how Edenred Italia manages its IT operations ensuring the security of processed information.

9.1. Operational procedures and responsibilities (organizational)

Edenred Italia has developed a set of documented procedures to regulate all key ICT activities which have a relationship with information security 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.

9.2. Change Management

Edenred Italia adopt a change management process and documented procedure for manage change request. Every change has: identified, recorded, planned, tested included fallback procedures, assessed from view point of impacted on service and security, approved with a formal process, communicated and managed in emergency mode if it need to resolve an incident


9.3. Capacity Management

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

9.4. Separation of development, testing and operational environment

Edenred Italia uses a separate environment for development, testing and operational.

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

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

9.5. Protection from malware (technical)

All workstations and malware-prone servers are equipped with an antivirus that the user cannot disable or change the configuration. The antivirus' update is centrally executed with an adequate frequency.

9.6. Backup (technical)

There are 2 different types of backup: complete backup, executed weekly, and incremental backup executed daily. Every weekend all backups are cloned and sent in a data bank for 4 weeks.

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

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

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 in a traffic light manner, 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 using Log Manager and the related evidence are stored for 6 months and periodically analyzed.

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.

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 autonomously install any software on them.

9.10. Information systems audit considerations (technical)

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

9.11. Clock Synchronization

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

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

10. Communications security

This chapter, traceable to ISO/IEC 27001 A.13, describes how Edenred Italia manages its networks ensuring the security of transmitted information.

10.1. Network security management (technical)

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

10.2. Information transfer (technical)

When necessary Edenred Italia 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.

.

10.3. Electronic messaging

Edenred Italia protect email messaging from unauthorized access, modification, denial of service, spam , phishing and any other attempted fraud. Edenred Italia account are protected, monitored and the security solutions used are updated periodically. Periodically Edenred carries out simulated phishing campaigns to test the efficiency of the systems and the effectiveness of the training and awareness-raising action

11. System acquisition, development and maintenance

This chapter, traceable to ISO/IEC 27001 A.14, describes how Edenred Italia securely maintains and evolves its information systems and software.


11.1. Security requirements of information systems (technical)

Edenred Italia 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 development personal is trained for secure coding periodically

11.2. Security in development and support processes (technical)

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

Software changes to Edenred Italia 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 change are tracked by centralized subversion platform and software code are reviewed by centralized security code analyzer for identification and fix bug or issue and intercept training opportunity.

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

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

11.3. Test data (technical)

Edenred Italia employs 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.

12. Supplier relationships

This chapter, traceable to ISO/IEC 27001 A.15, describes how Edenred Italia manages information security with its suppliers.

12.1. Information security in supplier relationships (organizational)

Standardized non-disclosure agreements with relevant suppliers are negotiated and included within their contracts. Additional information security-based considerations or service levels are applied on a case by case policy depending on the supplied services/goods included Cloud Service Provider

12.2. Supplier service delivery management (organizational)

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

13. Information security incident management

This chapter, traceable to ISO/IEC 27001 A.16, describes how Edenred Italia manages information security incidents


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

IT incident monitoring is continuously performed within Edenred Italia. 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.

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

14. Information security aspects of business continuity management

This chapter, traceable to ISO/IEC 27001 A.17, describes how Edenred Italia manages information security in situations where the business continuity is at stake.

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

14.1. Information security continuity (organizational)

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

14.2. Redundancies (technical)

A business continuity plan is present to prevent events that could stop the operation of Edenred Italia.

The plan focus on:

- Energy blackout: both short and long time.
- Inaccessible building.
- Air conditioning failure in the server room.
- Connectivity failures.
- Dual Datacenter Active/Active for Disaster Recovery

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

15. Compliance

This chapter, traceable to ISO/IEC 27001 A.18, describes how Edenred Italia manages compliance to the elements specifying effective information security requirements.

15.1. Compliance with legal and contractual requirements (organizational)

Edenred Italia annually revises its information security constraints within the scope of its ISO/IEC 27001 certification, considering applicable legal and contractual requirements.

15.2. Information security reviews (organizational)


Edenred Italia, being ISO/IEC 27001 certified, annually develops and carries out a program of both internal and external audit on those schemes, ensuring a constant third-party double control on information security.

15.3. Technical security reviews (organizational)

Edenred Italia periodically relies on specialized companies for an independent assessment of the security of its systems through 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

16. Data protection

This chapter, traceable to ISO/IEC 29151 Annex A, describes how Edenred Italia manages personal data protection related topics extending beyond information security.

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
	Status (first draft, reviewed, approved)	approved

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

Edenred Italia is developing a renewed privacy policy following the guidelines coming from applicable best practices that meets the requirements of the new Regulation.

16.2. Consent and choice (organizational)

All data processing consents proposed by Edenred Italia are being reviewed in light of the new Regulation, allowing the data subject to freely perform his/her choices for separate purposes where applicable. Data subjects are already being informed whether their consent is required to proceed with processing activities within all data protection notices, which are being exhaustively reviewed for compliance with the requirements of the new Regulation. This activity is being performed jointly while verifying the purpose legitimacy.

16.3. Purpose legitimacy and specification (organizational)

Edenred Italia is reviewing all bases for personal data processing being performed in order to have them aligned to the new Regulation and related requirements. This activity is being performed jointly while verifying required consents. Gathered bases are being inserted within the newly required record of processing activities.

Data protection notices are also being reviewed to ensure they provide accurate information about the purpose of collection and processing, in line with the Group's guidelines.

16.4. Collection limitation (organizational)

The revision of data protection notices is also regarding the amount of collected personal data, aiming to its minimization within all personal data processing activities. The collection of personal data belonging to special categories is being specifically reviewed with the intention to remove them wherever feasible.

16.5. Data minimization (organizational)


In addition to limiting the collection of personal data, Edenred Italia is also improving its activities to minimize 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.

16.6. Use, retention and disclosure limitation (organizational)

Edenred Italia is performing a review of 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.

Retention time is being systematically set accordingly to contractual and legal obligations and for a proportionate amount of time.

	Security and GDPR	
	Section: Technical and Organizational Measures	Versione: 2.2
	Classification: Public document	Data: 04/09/2019
Status (first draft, reviewed, approved)	approved	

16.7. Accuracy and quality (technical)

Edenred Italia 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.

16.8. Openness, transparency and notice (organizational)

The revision of data protection notices is also regarding the language used to write them in order to maximize its clarity to every data subject and providing clear information on Edenred Italia procedures, processes and means used for personal data processing.

Data protection notices are also being revised for a general alignment with the requirements of the new regulation, primarily but not exclusively focusing on the completeness of all the mandatory information.

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

16.9. PII principal participation and access (organizational)

Edenred Italia is improving its processes allowing the exercise of data subject's rights in order to make them more efficient and quicker from one side and to include new rights introduced by the Regulation.

Those processes include complaints and data breach notification management.

16.10. Accountability (organizational)

Edenred Italia is adopting a modified organizational structure, involving a formally designated Data Protection Officer, towards a state-of-the-art personal data protection objective.

New procedures are being introduced to evaluate the need of performing Data Protection Impact Assessment activities and to possibly guide their execution in line with applicable best practices. Supplier management is also being reinforced with new assurance procedures aiming to require sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the new Regulation and ensure the protection of the rights of the data subject.

Operations executed on personal data are being 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 the new Regulation is also being transversally planned for all Edenred Italia personnel.

16.11. Privacy compliance (organizational)

Edenred Italia 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. This program is still ongoing and is addressing several of the previous points, aiming to successfully conclude them in time for the new Regulation application.