CONDECO

General Data Protection Policy

Condeco Policy

Confidentiality Level: Public

Contents

Identification			
Title	General Data Protection Policy		
Type	Policy		
Code	PO.A18.02		
Origin	Internal		
Confidentiality Level	Public		
Language	English		
Publication Format	Electronic		
Publication Location	https://condecosoftware.sharepoint.com/employeeportal/Information Security Management System/A.18 Compliance		
Responsibility	**Name**		
Owner	IT Department		
Author(s)	Massimo Solari		
Reviewer(s)	Philip Briffa		
Approver	IT Governance Steering Committee		
Version	**Status**	**Reason for change**	**Date**
1.0	Released	Initial Release	21.07.2017
Distribution List			
Condeco Group Functions			

1. Introduction

Condeco is a multinational group organised in subsidiaries, with premises also included outside of the EEA.

Condeco is committed to maintaining its outstanding levels of Information Security and the same level of Data Protection amongst all its subsidiaries, and for every activity performed by the group.

Condeco is compliant with the EU General Data Protection Regulation (GDPR). GDPR was approved by the European Parliament on 14 April 2016 and replaces the European Directive (95/46/EC) on 25 May 2018, which was implemented in the United Kingdom (UK) by the Data Protection Act 1998. The GDPR will be directly applicable to the UK. Compliance with EU and UK data protection legislation is monitored, regulated and enforced by the Information Commissioner's Office (the UK's "supervisory authority"), which is responsible for promoting the protection of personal information.

Data Protection is a key activity inside Information Security. Condeco has two different Management Systems:

- An Information Security Management System (ISMS).
- A Personal Information Management System (PIMS).

A set of policies and procedures belonging to these two systems, dealing with data protection, are in place.

Condeco operates on Personal Data into two possible ways:

- As Data Controller, and
- as Data Processor.

As Data Controller, Condeco is responsible for the following sets of data:

- Condeco employees, contractors, visitors and equivalent personnel.
- Contact details for marketing and sales purposes.
- Suppliers data for administrative purposes.

The Personal Information Management System provides a framework for maintaining and improving compliance with data protection requirements and good practice. It is responsible for maintaining GDPR compliance for the above sets of data.

As Data Processor, Condeco is responsible for the following sets of data:

- Client data for Condeco SaaS service (room/desk booking services).

The Information Security Management System is responsible for maintaining GDPR compliance for this set of data.

The Condeco IT Governance Steering Committee rules on every issue concerning Information Security: it is committed to guarantee the respect of GDPR.

Users of this document are employees of Condeco (Condeco Group Ltd and Global subsidiaries), as well as every Data Subject with a potential interest in the correct application of these rules.

2. Reference documents

- DC.07.01 – ISMS Documentation
- PO.A05.01 – Information Security Policy
- PO.A18.01 – Compliance Policy
- DC.04.03 – PIMS Scope
- DC.04.01 – ISMS Scope

3. Definitions

This document adopts the definitions contained in the "EU Data Protection Regulation – Article 4 Definitions".

Hereinafter are reported the definitions more extensively used in this document:

Personal Data (or Personal Identifiable Information): any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Data (or Sensitive Personal Data or Special Categories of Personal Data): Personal Data, particularly sensitive, in relation to fundamental rights and freedoms. This personal data should include data revealing racial or ethnic origin, whereby the use of the term 'racial origin' does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races; political opinions, religious beliefs or other beliefs of a similar nature, whether the data subject is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), physical or mental health or condition, sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Natural person (data subject): is a living individual who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Biometric information: personal information resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person.

Genetic information: personal information relating to the inherited or acquired genetic characteristics of a natural person.

Personal information: information relating to an identified or identifiable natural person.

Personal Information Management System (PIMS): part of the overall management framework that plans, establishes, implements and maintains the management of personal information.

Profiling: form of automated processing of personal information consisting of the use of personal information to evaluate certain personal aspects relating to a natural person.

Consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Main establishment means:

a) with regards to a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case, the establishment having taken such decisions is to be considered to be the main establishment; and
b) with regards to a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor takes place to the extent that the processor is subject to specific obligations under this Regulation.

Binding corporate rules: personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers, or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Supervisory authority: an independent public authority, established by a Member State pursuant to Article 51.

Cross-border processing means either:

a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
b) processing of personal data, which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

4. Scope

As already stated, Condeco operates on Personal Data in two possible ways:

- as Data Controller;
- as Data Processor.

Data scopes are different in the two cases. Particularly:

- the scope as Data Controller is described in detail in the document "DC.04.03 – PIMS Scope". It covers the internal IT Infrastructure (SW and HW) and all Condeco branches;
- the scope as Data Processor is described in detail in the document "DC.04.01 – ISMS Scope". It covers the SaaS IT Infrastructure (SW and HW) and three Condeco branches: London and Newcastle (UK), Gurgaon (India).

As Data Controller, Condeco is responsible for these data sets:

- Condeco employees, contractors, visitors and equivalent personnel;
- customer data for marketing and sales purposes;
- supplier data for administrative purposes.

As Data Processor, Condeco is responsible for these data sets:

- Customers data for Condeco SaaS service (room/desk booking services).

In particular, in the first case (Data Controller), Condeco gathers data and then processes them. Both Personal Identifiable Information (PII) data and sensitive data are in the data set of which Condeco is responsible for.

In the second case (Data Processor), Condeco operates a cloud-based service for room and desk booking. PII data are directly inserted by Customers inside Condeco SaaS platform through a web/mobile application. Condeco simply (processes) stores Customer data inside a database. In this case, no sensitive data are processed or stored.

GDPR applies to all data, both the ones processed as Data Controller and as Data Processor.

As Data Controller, Condeco processes Personal Data for the following purposes:

- employees, contractors, visitors and equivalent personnel: accountability, finance, contractual liabilities and duties, government requirements, healthcare;
- customers data: marketing activities, accountability;
- suppliers data: accountability, finance, contractual liabilities and duties.

As Data Processor, Condeco processes Personal Data for the following purposes:

- customers data: delivery of SaaS service.

Hereinafter, the details of data processing are described accordingly with these two situations.

Data Controller

The Human Resources function processes Personal Data of employees, professional experts and consultants, visitors for the following purposes:

- Recruitment: personal data (including sensitive data) are collected, stored and analysed. It is possible that such information is transferred to line managers or other Condeco managers outside the EEA.
- Hiring: personal data (including sensitive data) are processed by line managers or other managers, also outside the EEA, in order to allow a new employee to access every facility, physical or technological.
- Administration: personal data (including sensitive data) are processed to accomplish with every legal obligation related to the administrative position of the employee (tax calculation and payment, pension scheme, insurances, etc …); data may be transferred outside the EEA.
- Statistics: personal data (including sensitive data) are processed in order to perform statistics studies on Condeco personnel in order to verify and/or improve internal policies (such as male/female employees, different nationalities, ageing, diversity, etc …). Data may be transferred to Condeco subsidiaries also outside the EEA.

Personal data is gathered, stored and processed to maintain company's accounts and records and to support and manage employees.

Examples of data processed include:

- Personal details
- Financial details
- Education details
- Employment details

Moreover, sensitive data may be processed as follows:

- Physical or mental health details
- Racial or ethnic origin
- Religious or other beliefs of a similar nature
- Trade union membership
- Offences and alleged offences

The Marketing function processes Personal Data of customers and/or enquirers, for the following purposes:

- Advertising: personal data (NOT sensitive data) are collected, stored and analysed to be used during campaigns.
- Market analysis: personal data (NOT sensitive data) are collected, stored and analysed for statistical purposes.

Personal data is gathered, stored and processed to advertise and promote our services.

Examples of data processed are as follows:

- Personal details
- Goods and services
- Family, lifestyle and social circumstances

During this activity, it is possible that personal data is transferred outside the EEA to other Condeco managers.

The Sales function processes Personal Data of customers, for the following purposes:

- Administration: personal data (including sensitive data) is collected and stored in order to accomplish contractual requirements. It is possible that such information is transferred to other Condeco managers outside the EEA.

Examples of data processed is as follows:

- Personal details
- Goods and services
- Financial details

Data Processor

SaaS Global Support function processes Customer Data to accomplish with the room/desk booking service and contractual requirements. No sensitive data is processed. Data belongs to customers, employees, consultants, visitors.

Condeco processes personal information to provide a service in which Condeco designs, tests, demonstrates and distributes software and hardware; provides an internet hosting service; as well as provideing an IT support and advice service.

5. Data Protection Principles

Condeco adheres to the GDPR's data protection principles. In particular, the GDPR requires personal information to be processed according to six data protection principles, which require personal information to be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are, in accordance with Article 89(1), not considered to be incompatible with the initial purposes ("purpose limitation");
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ("data minimisation");
d) accurate and, where necessary, kept up-to-date; every reasonable step is taken to ensure that personal information that is inaccurate, with regards to the purposes for which it is processed, is erased or rectified without delay ("accuracy");
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed; personal information can be stored for longer periods so far as the personal information is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject ("storage limitation"); and
f) processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

There is a seventh principle which requires data controllers to be accountable for, and be able to demonstrate compliance with, the six principles above.

6. Personal Information Management System

Condeco has decided to have in place, a Personal Information Management System (PIMS) in order to deal with personal data protection. PIMS has its own scope, but is fully integrated with Condeco ISMS. In particular, most of controls are shared between the two management systems.

The detailed scope of PIMS is described in the document "DC.04.03 – PIMS Scope". The list of selected controls for PIMS is described in the following documents:

- DC.06.10 – Data Protection Impact Assessment Report
- DC.06.11 – Data Protection Risk Treatment Plan

7. Data Protection Guidelines

Condeco Data Protection guidelines are as follows:

a) Data Protection must be appropriate to the purpose of the organization.
b) PIMS objectives will be defined by the IT Governance Steering Committee and inserted inside the document "DC.06.03 – Information Security Objectives".
c) GDPR applicable requirements shall be satisfied.
d) PIMS management system will be subject to the continual improvement methodology as described in the document "PO.10.01 – ISMS/PIMS Improvement Policy".

The current General Data Protection Policy:

- is available as documented information;
- is communicated within the organisation; and
- is available to interested parties, as appropriate.

Condeco is fully committed to comply with data protection requirements and good practice, including:

1) processing personal information only where this is strictly necessary for legal and regulatory purposes, or for legitimate organisational purposes;
2) processing only the minimum personal information required for these purposes;
3) providing clear information to natural persons about how their personal information can be used and by whom;
4) only processing relevant and adequate personal information;
5) processing personal information fairly and lawfully;
6) maintaining a documented inventory of the categories of personal information processed by the organisation;
7) keeping personal information accurate and, where necessary, up-to-date;
8) retaining personal information only for as long as is necessary for legal or regulatory reasons or for legitimate organisational purposes and ensuring timely and appropriate disposal;
9) respecting natural persons' rights in relation to their personal information;
10) keeping all personal information secure;
11) only transferring personal information outside the EEA and Switzerland in circumstances where it can be adequately protected;
12) where appropriate, the strategy for dealing with regulators across the EU, where goods and/or services are offered to natural persons who are resident in other EU countries;
13) the application of the various exemptions allowable by data protection legislation;
14) developing and implementing a PIMS to enable the PIMS policy to be implemented;
15) where appropriate, identifying internal and external interested parties and the degree to which they are involved in the governance of the organisation's PIMS;
16) the identification of workers with specific responsibility and accountability for the PIMS; and
17) maintain records of processing of personal information.

At Condeco, in order to gather, store and process Personal data for the above mentioned purposes, one of the following conditions must be satisfied:

- The data subject has unambiguously given his consent.
- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- The processing is necessary for compliance with a legal obligation to which the controller is subject.
- The processing is necessary for the purposes of the legitimate interests pursued by Condeco or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

8. Special Categories of Personal Data

When special categories of personal information are being processed, Condeco, in addition to the list detailed in paragraph seven, identify, define and document the additional legal basis for the processing of personal information. Such additional legal basis is selected from one or more of the following:

- natural person's explicit consent for specific purposes;
- necessary for employment rights or obligations;
- necessary for protecting the vital interests of the natural person;
- necessary for legitimate activities of a foundation, association, or any other non-profit making body for a political, philosophical, religious or trade union aim, with appropriate safeguards;
- information deliberately made public by the natural person;
- necessary for the establishment, exercise or defence of legal claims;
- necessary for reasons of substantial public interest;
- necessary for preventive or occupational medicine, assessment of the working capacity of an employee, medical diagnosis, provision of health or social care systems and services;
- necessary for reasons of public health or professional secrecy; and
- additional provisions for processing of a kind introduced by national laws with regards to the processing of genetic, biometric or health data.

9. Prior Consultation and Authorisation

Where risks to the natural person from personal information processing are identified by the Data Protection Impact Assessment (see "DC.06.10 - Data Protection Impact Assessment Report") to be of a high level, and the risks are unable to be mitigated, prior consultation and authorisation by the supervisory authority shall be sought.

Condeco has documented information on the criteria and processes for interacting with UK – Information Commissioner's Office (see "DC.A06.01 – Information Security Relevant Contacts") on prior consultation and authorisation.

10. Privacy by Design and by Default

When designing or making significant changes to:

a) systems for use within the organisation or by data processors; or
b) products and services for the use of individuals or other organisations, Condeco ensures that the processing of personal information by such systems, products or services:
    - is minimised by default;
    - uses de-identified information where possible; and
    - is transparent with regards to the functions and processing of personal information.

This is assured because Condeco has in place the appropriate organizational and technical actions:

1) that are appropriate to the risks identified;
2) that ensure privacy controls identified are implemented as appropriate personal information protections; and
3) that retain appropriate documented information of privacy by design activities and results.

11. Data Protection Officer (DPO)

The IT Governance Steering Committee has decided to appoint a Data Protection Officer (DPO) to deal with data protection issues and laws and regulations compliance. In particular, the Information Security Officer (ISO) has been appointed as DPO. DPO's primary tasks are as follows:

- inform and advise the IT Governance Steering Committee of Company's obligations;
- monitor compliance with EU-GDPR;
- provide advice with regards to the Data Protection Impact Assessments;
- to cooperate with ICO, if requested; and
- to represent a contact point with data subjects.

12. Transparency and information right

The Condeco General Data Protection Policy is published inside Condeco Information Security Management System documentation. It is classified as "PUBLIC" since it must be accessed by every person (data subject) interested to.

The document is available on the company's SharePoint platform. A copy of this policy is available to Public for consultation also on the Condeco website. According to the role played by Condeco, the document may be disclosed to the public in different ways.

Data controller: when Condeco operates as data controller the document is delivered as follows:

HR purposes: every employee and contractor are informed through a specific clause inside the contract. Such a clause must be specifically accepted. A signature is explicitly required as proof of acceptance. General Data Protection Policy is deployed after a person has been employed during the induction course. HR Director receives an acknowledgement when the document has been downloaded and read by the employee. Moreover, a specific awareness course is held through Condeco's LMS platform (Condeco Academy). Every employee is required to attend a GDPR awareness course. An effectiveness test is provided as well. Records are kept as evidence for auditing purposes.

Data subjects are provided at least with the following information.

- The identity of the controller and of his representative.
- The purposes of the processing for which the data is intended.
- Additional information such as:
    - the recipients or categories of recipients of the data, and
    - the existence of the right of access to and the right to rectify the data concerning data subject.

Condeco visitors are informed when they reach Condeco's premises. A formal consent to personal data processing is gathered. Details are contained in the following documents:

- PO.A09.01 – Access Control Policy
- PR.A09.07 – Access Control Procedure

Marketing purposes: every Condeco customer or enquirer is informed when accessing the Condeco website for the first time or when give the consent to personal data processing. A link to Condeco's General Data Protection Policy is available on Condeco website. Customers or enquirers may download a copy of the document.

Sales purposes: every Condeco customer is informed when he signs the contract or when give the consent to personal data processing. Also in this case a link to Condeco General Data Protection Policy is available on Condeco website. Customers may download a copy of the document.

Data processor: when Condeco operates as data processor the document is delivered only upon Customer's request. In particular, in this case personal data are not obtained directly by the data subject, but by Condeco customer. It is responsibility of customer to provide the document to the data subject. Nevertheless, Condeco is available to facilitate the delivery of the document through a specific link on its website.

13. Rights of access, rectification, erasure and blocking of data

Condeco is compliant with EU General Data Protection Regulation. As such, every right concerning Data Protection is guaranteed. In particular, every data subject has the right to:

- obtain without constraint at reasonable intervals and without excessive delay or expense a copy of all data relating to them that are processed;
- obtain the rectification, erasure or blocking of data in particular because the data are incomplete or inaccurate;
- object, at any time on compelling legitimate grounds relating to their particular situation, to the processing of their personal data, unless that processing is required by law. Where the objection is justified, the processing will cease; and
- object, on request and free of charge, to the processing of personal data relating to him for the purposes of direct marketing.

Specific tickets are available in order to:

- Retrieve personal data on an electronic media for archiving
- Transfer personal data to another data controller/data processor
- Delete every personal data
- Raise a formal compliant

At this purpose, Condeco has a specific page on its website for Infosecurity issues. Every data subject may access the following link http://www.condecosoftware.com/uk/informationsecurity/dataprotection/ and obtain information on specific issues.

Each compliant will be automatically addressed to the Condeco Data Protection Officer. Condeco Data Protection Officer will process the compliant and inform the IT Governance Steering Committee.

The IT Governance Steering Committee will evaluate every compliant even in the case it has already been solved.

Condeco General Data Protection Policy grants rights to data subjects to enforce the rules as third-party beneficiaries.

Data subjects can lodge claims before the jurisdiction of Condeco Headquarters (London, UK).

14. Automated individual decisions

Condeco does not process automatically Personal Data in order to take decisions or undertake actions relevant to a data subject. Any individual decision on a data subject is taken through a manual process involving at least two different managers.

Automated personal data processing is allowed only for back office operations, statistical purposes or to accomplish with service requirements.

15. Security and confidentiality

Condeco has an Information Security Management System compliant with ISO 27001:2013 standard and a Personal Information Management System compliant with BS 10012:2017. A Risk Analysis process is in place. The main business processes have been analysed to identify and classify the relevant information according to three attributes:

- Confidentiality
- Integrity
- Availability

Personal Data is amongst the information that is classified as HIGH in the Risk Analysis. According with the Risk Analysis methodology, if information is classified as HIGH, then every asset (HW, SW, people, facility) supporting such information is also classified as HIGH. According with this principle, the assets supporting Personal Data have been carefully analysed and controls have been selected in order to mitigate the associated risks. Controls have been selected from the ones contained and recommended in the ISO 27002:2013 standard.

A full description of the Risk Analysis process, the findings, the chosen controls and their implementation is contained inside the ISMS/PIMS documentation. The following document "DC.07.01 – ISMS/PIMS Documentation" contains the list of all the ISMS/PIMS document grouped according to the Control Objectives defined by the ISO 27002:2013 standard. The document is classified as PUBLIC and is available at the following link http://www.condecosoftware.com/uk/informationsecurity/dataprotection/.

A more detailed description of the technologies in use and the countermeasures adopted to minimise the risk for the protection of personal data may be found in the following documents:

- DC.06.10 – Data Protection Impact Assessment Report;
- DC.06.11 – Data Protection Risk Treatment Plan.

16. Training programme

Condeco has a specific training and awareness programme for Information Security as required by ISO 27001 and BS 10012. A course catalogue is available.

Awareness courses must be attended by all the employees and contractors.

A specific course on GDPR is available.

Every course is provided through Condeco's LMS platform, Condeco Academy.

Thanks to such a platform, every participant is tracked, and a final test is inserted at the end of the course in order to understand the effectiveness of the programme.

Induction courses are also available for new employees.

The Condeco Academy may also be accessed by customers and suppliers (only limited courses). Particularly, the course on GDPR is available to external processors.

The training programme is regularly reviewed and updated on an annual basis.

Auditing activities are regularly carried on at least on annual basis.

17. Audit programme

Condeco has a specific Internal Audit Programme to check and maintain compliance against a number of requirements:

- ISO 27001:2013
- GDPR
- CSA_CCM_v.3.0.1
- BS 10012:2017

The internal audit programme covers all aspects of the GDPR. It is regularly reviewed on an annual basis.

Internal audits are planned at least twice a year. Every Condeco subsidiary is subject to internal audits.

Moreover, Condeco is certified according to ISO 27001. Every year Condeco has different 3rd party audits performed by the Certification Body's assessors.

The results of both internal and external audits are discussed inside Condeco's IT Governance Steering Committee. For each non-conformity and/or observation an Information Security incident ticket is raised on ServiceNow, the Condeco platform for incident and problem management.

An abstract of the Audit report is available to the UK Information Commissioner's Office upon request: the full report is never made available as it can contain security critical data.

Second party audits are allowed and welcome.

Particularly:

- Data Protection Authorities have the power to carry out a data protection audit if required.
- Each Member of the Condeco Group accepts that he could be audited by the Data Protection Authorities.

18. 18. Compliance and supervision of compliance

At Condeco, the IT Governance Steering Committee is in charge to properly address every issue concerning Information Security.

The IT Governance Steering Committee has been established to accomplish the following tasks:

- Establish and operate an ISMS compliant with the ISO/IEC 27001:2013 standard.
- Establish and operate an PIMS compliant with the BS 10012:2017 standard.
- Define the Information Security Objectives.
- Define ISMS/PIMS Policies and Procedures.
- Provide the resources necessary to ISMS/PIMS.
- Integrate the ISMS/PIMS inside the other Condeco business processes.
- Train personnel and suppliers and communicate the ISMS/PIMS obligations/liabilities to the relevant parties.
- Establish roles and responsibilities.

The IT Governance Steering Committee operates both ISMS and PIMS, as defined in the Condeco ISMS and PIMS Scope Documents.

Directives established by the IT Governance Steering Committee apply to all staff working at Condeco in whatever capacity.

It represents the Executive Body as concerns every IT Governance and Information Security issue at Condeco.

It is formed by the most relevant Condeco Directors leading critical functions inside the ISMS Scope. The IT Governance Steering Committee is formed by the following permanent members:

- Chief Financial Officer
- Global Support Director
- IT Director
- R&D Director
- HR Director
- Information Security Officer

Among the responsibilities of the IT Governance Steering Committee is to assure that every Condeco subsidiary is compliant with GDPR.

19. Validity and document management

This document is valid as of 21 July 2017.

The owner of this document is the IT Department, who must check and, if necessary, update the document at least on a yearly basis.

Our Global Reach

London | Frankfurt | Munich | Paris | Stockholm | Zurich | Dubai
New York | San Jose | Singapore | Sydney | Hong Kong | Gurgaon