Privacy Policy

Date	October 19th, 2022
Status	APPROVED and EFFICTIVE
Version	2.2
Purpose	Provide an internal policy document regarding the privacy of data
Scope	ORTEC

Version history

Version	Date	Changes	Modified by
1.0	2018-10-08	Approved by Executive Team ORTEC	
1.1	2019-02-26	Art.4 – modified 'information' into 'Personal Data' Art.5.3 – modified publication location to QRC SharePoint site	
1.2	2019-05-08	Added new article (5.4) on Privacy Champions	
1.3	2020-08-10	Modified document to include other legislation beside GDPR	
1.4	2020-10-22	Grammar check throughout document. Art. 4 – last paragraph: modified territorial scope of data transfers Art.5.1 – Modified role description: removed responsible role for the Executive Team Art.5.8 – added role definition for development	
1.9	2020-10-28	Approved by ISC	
2.0	2020-11-09	Approved by ET	
2.1	2021-10-08	Reviewed – no adjustments	
2.2	2022-10-19	Reviewed – No changes needed	

Table of contents

1 Motivation and purpose

ORTEC strives to be a reliable employer and business partner. We aim to secure our own data and information as well as that of our customers in correspondence with applicable laws, regulations and generally accepted standards. For all data and information, but especially for Personal Data this means dealing with this data in a responsible manner, to mitigate the risk that Privacy sensitive data potentially holds.

The goal of this Privacy Policy is to ensure that all ORTEC employees are aware of ORTEC's views concerning privacy. This policy addresses how ORTEC will treat the data of employees, customers, visitors as well as users of the ORTEC website.

This policy is compliant with the current privacy legislation (eg. GDPR, LGPD) and should be interpreted together with the ORTEC Privacy Statement, ORTEC General Information Security Policy and the ORTEC Information Classification Policy.

2 Scope

For this policy, 'information' is interpreted as: all internal Personal Data in digital form as well as on paper, as well as Personal Data received from or sent to external parties in digital form as well as on paper.

For the remainder of this Policy the term 'Personal Data' will be used.

This policy applies to all employees of ORTEC, including all its subsidiaries and joint ventures where ORTEC a) owns 50% or more of the company and/or b) has managerial control , and to all Personal Data that is processed within ORTEC including all its subsidiaries and joint ventures where ORTEC a) owns 50% or more of the company and/or b) has managerial control.

3 Support within the organization

This document and all other information security and privacy documents are fully supported by the management of ORTEC. This Privacy Policy document will be the starting point for all other documents concerning privacy, including the privacy statement published on the ORTEC website.

ORTEC's responsibility towards privacy is translated in several technical and organizational measures and guidelines. ORTEC aims to be as transparent as possible in these towards our employees and customers. To support this transparency ORTEC maintains a Processing Registry, providing information as well as forming the foundation for the whole organization on why, when and by whom Personal Data is processed.

4 Use of personal data

ORTEC uses Personal Data at all levels within the organization, in different ways and with different purposes. ORTEC will determine the appropriate lawful base for processing for each activity, and document this in the processing registry. If the regular legal bases are not applicable, ORTEC will use the legal base of ‘consent’ to comply to privacy legislation such as GDPR and LGPD.

ORTEC may share customers’ Personal Data with third parties and services only after agreement of the customer using the Data Processing Agreement. ORTEC has Data Processing Agreements with all third parties with which personal data is exchanged.

Where Personal Data is shared with third parties ORTEC will make sure the level of security and privacy provided by the third party is similar to the levels practiced at ORTEC. In transferring Personal Data ORTEC will follow applicable privacy legislation if and where necessary. For cases where Personal Data is shared outside of the country/region the data originates from, for example outside the European Economic Area (EEA) for European customers, the need for additional safeguards will be determined on a case-by-case basis.

5 Roles and responsibilities

5.1 Executive Team

ORTEC’s Executive Team is accountable for organizing privacy at ORTEC by defining and enabling a privacy organization, including required roles and resources, policies, and follow-up. As such, the Executive Team is also accountable for the processing of Personal Data to be conducted in a legitimate manner.

The Executive Team assigns and delegates responsibilities to the resources of the privacy organization and is responsible for approving the general security and privacy policies of ORTEC.

The Executive Team will be notified of major data breaches that could have a significant impact on the ORTEC organization and/or its reputation.

5.2 Information Security Committee

The Information Security Committee (ISC), as defined in the Information Security Roles and Responsibilities document, advises, evaluates, and approves policies and guidelines concerning Information Security and Privacy.

5.3 Data Protection Officer

ORTEC has assigned a Data Protection Officer (DPO) as an independent global advisor for privacy-related matters. The role of DPO is explained in depth in the Data Protection Officer document that is published via the SharePoint page of the QRC Team, defining responsibilities and tasks.

Main tasks/responsibilities of the DPO include, but are not limited to:

- Advising Executive Team, country managers, managers, employees and third parties about their duties regarding the GDPR.
- Ensuring, monitoring, and reporting compliancy with Privacy legislation globally, such as for example the GDPR (EEA) and the Australian Privacy Act, and the processing activities of ORTEC.
- Maintain framework of all processing activities (for example the Processing Registry and Privacy Impact Assessments) of ORTEC, as well as a framework for registration of all Privacy related incidents, such as data leaks and all follow up actions.
- Responsible for managing privacy related incidents such as data leaks and all follow up actions.
- Be the contact point for Data Protection Authorities
- Work together with the Data Protection Authority on all issues regarding Privacy, such as data leaks and audits.
- Continuously improving policy, procedures, and registration of privacy-related matters.
- Creating awareness and educate employees on privacy-related matters.

5.4 Privacy Champions

ORTEC has assigned local Privacy Champions to work together with the DPO on matters that are privacy related. The tasks/responsibilities of the Privacy Champion are published via the QRC Team SharePoint site, in the Privacy section.

The main responsibilities of a privacy champion include, but are not limited to:

- Local point of contact for privacy related matters
- Provides input for the Processing Registry
- Assists with Data protection Impact Assessments (DPIA)
- Reviews Data Processing Agreements (DPA)

5.5 Managers/supervisors

Managers/supervisors (hereafter referred to as managers) are responsible for informing their subordinates on this Privacy Policy, and any policies derived from it.

Managers are also responsible for ensuring their subordinates comply with this Privacy Policy, as well as with procedures and processes regarding privacy.

Managers are responsible to create and improve awareness on Privacy and Information Security by making Privacy and Information Security a topic during department meetings, team meetings, personal evaluations, etc.

Managers are responsible for monitoring compliancy of their subordinates to the Privacy Policy and any policies and guidelines derived from it, as well as the behavior of these subordinates. The managers are responsible for reporting deviations to the DPO.

5.6 Process Owner

The Process Owner is the party that determines the goal and the company assets involved in processing the Personal Data: it must be clear at all times who is the responsible party. Process Owners are registered in the Processing Registry.

The Process Owner is responsible for the Processing Registry entries and provides input to the DPO regarding the Processing Registry. The Process Owner is also responsible to keep the Processing Registry up to date.

The Process Owner is responsible for implementing and monitoring processes compliant to the processing registry and legislation. The Process Owner is responsible for reporting deviations to the DPO.

The Process Owner is responsible for the privacy requirements and measures of new processing activities and changes to existing processing activities and conducts a Privacy Impact Assessment (PIA).

5.7 Corporate IT

The Corporate IT Department is responsible for implementing and maintaining the technical measures related to Privacy and Security. They are responsible to translate the functional and privacy requirements into technical solutions. In doing so they have to practice ‘Privacy and Security by Default’ and ‘Privacy and Security by Design’. This means that both Privacy and Security are a mandatory requirement and need to be addressed from the start of each project. Throughout the project Privacy and Security need to be observed and taken into account, for example in case of changes to functionality.

Corporate IT is responsible for monitoring and logging of the technical systems and taking appropriate measures in case of abnormalities. For this they work together with the Security Officer, the DPO and the Information Security Committee.

Corporate IT is responsible for identifying deviations to Privacy and Security policies (for example in logging, project requirements, changes, etc.) and reporting them to the Information Security Committee directly, or via the DPO or Security Officer.

5.8 Development

The development of Data Science products and solutions is core business of the ORTEC organization. During development ORTEC strives to follow and comply to the principles of Security and Privacy by design and Security and Privacy by default.

Product Managers are responsible for the security and privacy requirements related to the ORTEC products and solutions. They are responsible for providing functionality in the ORTEC Products/Solutions to supports these requirements.

Team leads and managers are responsible for the methods and processes used for the development activity and the employees. Additional training is offered to employees in development roles to keep them up to date and informed. During the development phase only dummy data is used, for example for testing, unless approval is obtained from the customer.

5.9 Security Incident Response Team

The Security Incident Response Team (SIRT), as defined in the Information Security Roles and Responsibilities document, is responsible for handling all security incidents. If an incident concerns Privacy and/or Personal Data, the SIRT will involve the DPO to manage the privacy aspects of the incident.

5.10 Employees

The employee has a responsibility in familiarizing him/herself with all Information Security and Privacy related matters, such as but not limited to policies, guidelines, code of conduct, procedures, etc.

Employees are obligated to take part in the Security Awareness campaigns and trainings facilitated by ORTEC.

The employee is also responsible for reporting any incident, either Privacy or Information Security related. Reporting such an incident must be done using an IT Helpdesk request in Synergy.

6 Disciplinary measures

Violations of the Privacy Policy and all policies, guidelines and procedures derived from it, as well as violations of the Information Security Policy and all policies, guidelines and procedures derived from it, will be evaluated on a case-to-case basis, and may lead to disciplinary measures.

7 Continuous process

This Policy, the Processing Registry and all measures, procedures or guidelines deriving from it will be evaluated and, if necessary, adapted periodically (annually) to reflect the situation at time of evaluation, and in order to comply to the regulation and legislation that apply at time of evaluation by the Data Protection Officer.

The Data Protection Officer will ensure that any necessary improvements will also take place in the interim of the evaluation moments and will offer advice to the management at their request or when necessary.