Thoropass™

# GDPR Self- Assessment Compliance Report

## A Review of Thoropass's Compliance Against the General Data Protection Regulation (GDPR) (version 1.0)

**April 14, 2023; Reviewed/Updated April 16, 2024**

**Mailing Address:**
228 Park Ave S., PMB 41082,
New York, NY 10003

Thoropass™

# Table of Contents

# 1 Introduction

## 1.1 Background

The General Data Protection Regulation (GDPR) was made effective on May 25, 2018 imposing strict requirements on organizations to protect privacy and security of data subjects within the European Union (EU). This law encompasses seven (7) protection and accountability principles as well as data security.

## 1.2 Overview

This GDPR Compliance Report consists of a self-assessment performed by an experienced and qualified assessor during the review period of April 11, 2023 to April 14, 2023, reviewed/updated April 16, 2024.

Without defined policies and privacy over information systems, Thoropass's ability to conduct business may be impacted. The preservation of Thoropass's reputation is directly linked to the management over the privacy of Thoropass's information. Thoropass's primary concern related to privacy is the use and disclosure of personal data.

## 1.3 Objectives

The objective of this review was to verify Thoropass's policies, standards, and procedures meeting the objectives outlined in the GDPR. In addition, the objective of this review was to verify Thoropass's management and employees ensure appropriate compliance with the articles outlined in the GDPR.

## 1.4 Data Controller/Data Processor

Thoropass is considered a Data Processor under the provisions of GDPR as follows: Thoropass offers a compliance software-as-a-service platform to customers with a hybrid approach to include compliance experts to assist customers along their compliance journey. (See https://thoropass.com for additional information).

Thoropass processes (or performs any actions on data, whether automated or manual, such as collecting, recording, organizing, structuring, storing, using, resetting, or etc.) personal data on behalf of a data controller.

## 1.5 EU-US DPF

Thoropass, Inc. is posted on the Data Privacy Framework List located here: https://www.dataprivacyframework.gov/s/participant-search

Thoropass complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Thoropass has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Thoropass has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view Thoropass's certification, please visit https://www.dataprivacyframework.gov/s

Thoropass is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Thoropass is held liable in cases of onward transfers to third parties.

**Contact Information**
If an organization has any questions, comments, or concerns about Thoropass's privacy policy (https://thoropass.com/privacy-policy/) or their personal information, they can contact: privacy@thoropass.com. Thoropass's mailing address is 228 Park Ave S, PMB 41082, New York, NY 10003, United States.

**Independent/Alternative Dispute Resolution Provider**
Thoropass maintains an independent/alternative dispute resolution provider designed to address complaints and provide appropriate recourse free of charge to individuals from an alternative dispute resolution provider based in the U.S. If an individual believes their concerns were not addressed by contacting Thoropass directly, they can contact The International Centre for Dispute Resolution® (ICDR®) (the international division of the American Arbitration Association® (AAA®)) at https://go.adr.org/privacyshield.html to file a complaint. An individual can also file a case by mail or email completing the appropriate Notice of Arbitration Form and forwarding it to the International Centre for Dispute Resolution:

International Centre for Dispute Resolution Case Filing Services
1101 Laurel Oak Road, Suite 100
Voorhees, NJ 08043
United States Phone: +1.212.484.4181
Email box: casefiling@adr.org

Thoropass provides the possibility, under certain conditions, for individuals to invoke binding arbitration.

# 2 Executive Summary

Overall, Thoropass's compliance posture with the GDPR meets compliance requirements to protect Thoropass's information systems and personal data. Thoropass has no items to report or consider. Section 3 provides details of this report and Section 2.4 provides a summary.

## 2.1 Scope

This assessment reviewed the use, disclosure, and accessibility of personal data available to authorized individuals. This assessment reviewed the articles of the GDPR summarized under Section 2.4 below.

The scope of this review included:

- The Thoropass's policies and procedures related to GDPR Compliance.
- The Thoropass's information system and platform maintaining personal data to include cloud hosting environment(s): Amazon Web Services (AWS)
- This assessment include the following location: 159 W 25th Street, New York, NY 10001

## 2.2 Methodology

Thoropass conducted a process-based review focusing on the significant objectives of GDPR compliance. Thoropass reviewed the eleven (11) chapters and ninety-nine (99) articles documented in the GDPR. Thoropass utilized these articles to collect evidence in sufficient quantity/quality to validate conformity. The use of these procedures provide a systematic way to perform assessments reducing the risk of errors and reinforcing the objectivity of the assessment's conclusions. Recommendations were provided according to regulatory requirements, standards, frameworks, industry best practices, and experience from subject matter experts.

This assessment covers the seven (7) privacy protection and accountability principles outlined in the GDPR articles to include:

1. Lawfulness, fairness, and transparency: processing personal data lawfully, fairly, and in a transparent manner in relation to the data subject;
2. Purpose Limitation: collecting personal data for a specific, explicit, and legitimate purpose and not processing it further in a manner that is not compatible with the original purpose;
3. Data Minimization: ensuring personal data will be adequate, relevant, and limit to what is necessary in relation to the purpose for which it is processed;
4. Accuracy: ensuring personal data will be accurate and kept up to date as necessary; ensuring inaccurate personal data will be erased or rectified without delay;

5. Storage Limitation: ensuring personal data will be kept in a form which permits identification of data subjects no longer than is necessary for the purpose of processing;
6. Integrity and Confidentiality: processing personal data in a manner to ensure appropriate security over the personal data including protection against unauthorized (or unlawful) processing as well as against accidental loss, destruction, or damage using appropriate technical/organizational measures;
7. Accountability: ensuring the organization will be responsible to demonstrate compliance with GDPR requirements.

## 2.3 Findings and Recommendations

There were no findings or items of concern identified during this review in need of improvements.

## 2.4 Overall Summary

The GDPR regulations were assigned a compliance status defined as follows:

- **Applicable** - The regulation applies to Thoropass, but there isn't evidence required to prove compliance.
- **Fully Compliant** - Thoropass meets all criteria of the requirement.
- **Partially Compliant** - Thoropass meets some criteria of the requirement, but needs to improve compliance efforts based on the recommendations provided.
- **Not Compliant** - Thoropass does not meet the criteria of the requirements; recommendations are provided for consideration.
- **Not Applicable (N/A)** - the regulation doesn't apply to Thoropass.

The following table provides a summary of Thoropass's compliance status against the GDPR requirements:

| Articles | Status |
|---|---|
| **Chapter 1 General Provisions** | |
| 1-4 (Articles dealing with Scope and Definitions) | Applicable |
| **Chapter 2 Principles** | |
| 5 Principles Relating to Processing of Personal Data | Fully Compliant |
| 6 Lawfulness of Processing | Fully Compliant |
| 7 Conditions for Consent | Fully Compliant |
| 8 Conditions Applicable to Child's Consent in Relation to Information Society Services | Not Applicable |
| 9 Processing of Special Categories of Personal Data | Not Applicable |

| | |
|---|---|
| 10 Processing of Personal Data Relating to Criminal Convictions and Offenses | Not Applicable |
| 11 Processing which Does Not Require Identification | Not Applicable |
| **Chapter 3 Rights of the Data Subject** | |
| 12 Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject | Fully Compliant |
| 13 Information to be Provided Where Personal Data are Collected from the Data Subject | Fully Compliant |
| 14 Information to be Provided Where Personal Data Have Not Been Obtained from the Data Subject | Fully Compliant |
| 15 Right of Access by the Data Subject | Fully Compliant |
| 16 Right to Rectification | Fully Compliant |
| 17 Right to Erasure (Right to be Forgotten) | Fully Compliant |
| 18 Right to Restriction of Processing | Fully Compliant |
| 19 Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing | Fully Compliant |
| 20 Right to Data Portability | Fully Compliant |
| 21 Right to Object | Fully Compliant |
| 22 Automated Individual Decision-Making, Including Profiling | Not Applicable |
| 23 Restrictions | Fully Compliant |
| **Chapter 4 Controller and Processor** | |
| 24 Responsibility of the Controller | Fully Compliant |
| 25 Data Protection by Design and by Default | Fully Compliant |
| 26 Joint Controllers | Fully Compliant |
| 27 Representatives of Controllers or Processors Not Established in the Union | Not Applicable |
| 28 Processor | Fully Compliant |
| 29 Processing Under the Authority of the Controller or Processor | Fully Compliant |
| 30 Records of Processing Activities | Fully Compliant |
| 31 Cooperation with the Supervisory Authority | Fully Compliant |
| 32 Security of Processing | Fully Compliant |
| 33 Notification of a Personal Data Breach to the Supervisory Authority | Fully Compliant |
| 34 Communication of a Personal Data Breach to the Data Subject | Fully Compliant |

| | |
|---|---|
| 35 Data Protection Impact Assessment | Fully Compliant |
| 36 Prior Consultation | Fully Compliant |
| 37 Designation of the Data Protection Officer | Fully Compliant |
| 38 Position of the Data Protection Officer | Fully Compliant |
| 39 Tasks of the Data Protection Officer | Fully Compliant |
| 40-43 Code of Conduct/Certifications (Not applicable since these are still being worked on and approved by the EU) | Not Applicable |
| **Chapter 5 Transfers of Personal Data to Third Countries or International Authorities** | |
| 44 General Principle for Transfers | Fully Compliant |
| 45 Transfers on the Basis of an Adequacy Decision | Fully Compliant |
| 46 Transfers Subject to Appropriate Safeguards | Fully Compliant |
| 47 Binding Corporate Rules | Not Applicable |
| 48 Transfers or Disclosures Not Authorized by Union Law | Not Applicable |
| 49 Derogations for Specific Situations | Fully Compliant |
| 50 International Cooperation for the Protection of Personal Data | Not Applicable |
| **Chapter 6 Independent Supervisory Authorities** | |
| 51-59 (Articles related to supervisory authorities) | Not Applicable |
| **Chapter 7 Cooperation and Consistency** | |
| 60-76 (Articles related to cooperation and consistency between supervisory authorities) | Not Applicable |
| **Chapter 8 Remedies, Liability and Penalties** | |
| 77-84 (Articles related to remedies, liabilities, and penalties) | Not Applicable |
| **Chapter 9 Provisions Relating to Specific Processing Situations** | |
| 85-88 (Articles related to specific processing) | Not Applicable |
| 89 Safeguards and Derogations Relating to Processing for Archiving Purposes in the Public interest, Scientific or Historical Research Purposes or Statistical Purposes | Fully Compliant |
| 90-91 (Articles related to specific processing) | Not Applicable |
| **Chapter 10 Delegated Acts and Implementing Acts** | |
| 92-93 (Articles related to delegated acts and implementing acts) | Not Applicable |
| **Chapter 11 Final Provisions** | |
| 94-99 (Articles related to the final provisions of GDPR) | Not Applicable |

# 3 Report Details

## Chapter 1 General Provisions

### Article 1-4 Articles Related to Scope and Definitions

| Applicable | **Evidence:** PT-03 PII Processing Purposes (Purpose / Limitation / Legal Basis) |
|---|---|

**Regulation:**
See Appendix C for additional information.

**Observations/Findings:**
Thoropass processes personal data (wholly or in part) by automated means in order to form a filing system.

Thoropass is not established in the European Union (EU); however, it offers goods (or services) in the EU. Thoropass is required and contractually obligated to comply with the GDPR.

Thoropass incorporates the definitions of the GDPR within its policies/procedures.

Thoropass is considered a processor under the GDPR.

**Recommendations:** No further recommendations at this time.

## Chapter 2 Principles

### Article 5 Principles Relating to Processing of Personal Data

| Fully Compliant | **Evidence:** PT-03 PII Processing Purposes (Purpose / Limitation / Legal Basis); PT-05 Privacy Notice (Transparency); SI-12 Data Handling, Retention, and Disposal; PM-22 PII Quality Management; PM-21 Accounting of Disclosures; SC-08 Transmission Confidentiality and Integrity |
|---|---|

**Regulation:**
Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
- 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 shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be 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 organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
- processed in a manner that ensures appropriate security of the personal data, including protection against

unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').
- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

**Observations/Findings:**
Thoropass incorporates all seven (7) privacy principles within its Privacy Policies and Procedures to include: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

**Recommendations:** No further recommendations at this time.

## Article 6 Lawfulness of Processing

Fully Compliant | **Evidence:** PT-03 PII Processing Purposes (Purpose / Limitation / Legal Basis)

**Regulation:**
Processing shall be lawful only if and to the extent that at least one of the following applies:
- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- 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;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: Union law; or Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offenses are processed, pursuant to Article 10;
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

**Observations/Findings:**
Thoropass lawfully processes personal data under the following:
- Individual gives consent to processing for one or more specific purposes;

- Processing is necessary to perform a contractual obligation for the individual who is a party to the contract or in order to take steps at the request of an individual to enter into a contract; and
- Meet compliance with legal obligations.

**Recommendations:** No further recommendations at this time.

## Article 7 Conditions for Consent

| Fully Compliant | **Evidence:** PT-04 Consent (Individual Participation / Choice / Opt-In / Opt-Out); Consent Evidence |
|---|---|

**Regulation:**
Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

**Observations/Findings:**
Thoropass obtains consent from an individual to process their personal data. Thoropass also maintains withdrawals of consent as required. Written consent is present to individuals in an intelligible manner being easily accessible as well as written in clear and plain language.

**Recommendations:** No further recommendations at this time.

## Article 8 Conditions applicable to Child's Consent in Relation to Information Society Services

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.
Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.
Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

**Observations/Findings:**
Not applicable. Thoropass does not solicit goods or services to children under sixteen (16) years of age.

**Recommendations:** Not applicable.

## Article 9 Processing of Special Categories of Personal Data

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Paragraph 1 shall not apply if one of the following applies:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

**Observations/Findings:**
Not applicable. Thoropass does not process the following personal data:

- Data revealing racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or

| |
|---|
| • Data concerning an individual's sex life or sexual orientation. |
| **Recommendations:** Not applicable. |

## Article 10 Processing of Personal Data Relating to Criminal Convictions and Offenses

| | |
|---|---|
| Not Applicable | **Evidence:** N/A |
| **Regulation:**<br>Processing of personal data relating to criminal convictions and offenses or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority. | |
| **Observations/Findings:**<br>Not applicable. Thoropass does not process data related to criminal convictions or offenses. | |
| **Recommendations:** Not applicable. | |

## Article 11 Processing which Does Not Require Identification

| | |
|---|---|
| Not Applicable | **Evidence:** N/A |
| **Regulation:**<br>If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.<br><br>Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification. | |
| **Observations/Findings:**<br>Not applicable. The processing of personal data performed by Thoropass does not require the identification of an individual. Thoropass is not obligated and does not maintain, acquire, or process additional information to identify the individual. | |
| **Recommendations:** Not applicable. | |

# Chapter 3 Rights of the Data Subject

## Article 12 Transparent Information, Communication, and Modalities for the Exercise of the Rights of the Data Subject

| | |
|---|---|
| Fully Compliant | **Evidence:** PT-05 Privacy Notice (Transparency); Privacy Notice |
| **Regulation:**<br>The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any | |

communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- refuse to act on the request.
- The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardized icons.

**Observations/Findings:**
Thoropass provides a written privacy notice in a concise, transparent, intelligible, and easily accessible form using clear and plain language. Thoropass permits the exercise of individual rights as well as acts upon individual requests within one (1) month of receipt of request. Any delays are communicated to individuals and Thoropass will respond in no more than two (2) additional months on a request. Thoropass provides a determination of action such as not acting to a request within one (1) month along with instructions on how to lodge a complaint with a supervisory authority. Thoropass will provide communications and actions taken free of charge unless the request was found to be excessive or repetitive. Thoropass will confirm the identity of an individual (as may be necessary) and may provide information in a standard way utilizing icons that are machine-readable. *Note: Thoropass has not received any privacy related requests from any individuals in the last twelve (12) months.*

**Recommendations:** No further recommendations at this time.

## Article 13 Information to be Provided Where Personal Data are Collected from the Data Subject

| Fully Compliant | **Evidence:** PT-05 Privacy Notice (Transparency); Privacy Notice |
|---|---|

**Regulation:**
Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal

data are obtained, provide the data subject with all of the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

**Observations/Findings:**

Thoropass, at the time personal data is collected, provides individuals with required information such as:

- The identity and the contact details of Thoropass and Thoropass's representative, where applicable;
- The contact details of the data protection officer, where applicable;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- Thoropass doesn't process data based on legitimate interest;
- Thoropass doesn't share or transfer personal data and does not intend to transfer personal data to a third country (or international organization).

Thoropass will also provide the following to further ensure fair/transparent processing:

- Thoropass stores personal data for the duration of a customer's contract or for just as long as the personal data is needed.
- Thoropass maintains processes for the following rights: access to, rectification, erasure, restriction, or objection to processing as well as the right to data portability;
- When processing is based on consent, Thoropass maintains the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with a supervisory authority;
- Whether the provisions of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract as well as whether the individual is obliged to provide the personal data and the possible consequences of failure to provide such data;
- Thoropass does not utilize any automated decision-making solution or performs any profiling on individuals; and
- Thoropass does not intend for further processing of personal data other than what it was originally collected for; however, Thoropass will provide the individual with additional information on the purpose for this further processing if Thoropass does further process

| |
|---|
| personal data other than what it was originally collected for. |
| **Recommendations:** No further recommendations at this time. |

## Article 14 Information to be Provided Where Personal Data Have Not Been Obtained from the Data Subject

| | |
|---|---|
| Fully Compliant | **Evidence:** PT-05 Privacy Notice (Transparency); Privacy Notice |

**Regulation:**

Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The controller shall provide the information referred to in paragraphs 1 and 2:

- within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

Paragraphs 1 to 4 shall not apply where and insofar as:

- the data subject already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

**Observations/Findings:**

Thoropass provides individuals with required information if it is collected from a source other than the

individual such as:

- The identity and the contact details of the organization and the organization's representative, where applicable;
- The contact details of the data protection officers, where applicable;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- Categories of personal data;
- The recipients or categories of recipients of the personal data, if any; or
- Where applicable, the fact the organization intends to transfer personal data to a third country (or international organization) and the existence or absence of an adequacy decision, reference to the appropriate or suitable safeguards as well as the means by which to obtain a copy of them (or where they have been made available).

Thoropass will also provide the following to further ensure fair/transparent processing:

- Thoropass stores personal data for the duration of a customer's contract or for just as long as the personal data is needed.
- Thoropass maintains processes for the following rights: access to, rectification, erasure, restriction, or objection to processing as well as the right to data portability;
- When processing is based on consent, Thoropass maintains the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with a supervisory authority;
- Whether the provisions of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract as well as whether the individual is obliged to provide the personal data and the possible consequences of failure to provide such data;
- From which source the personal data originated, and if applicable, whether it came from publicly accessible sources; or
- Thoropass does not utilize any automated decision-making solution or performs any profiling on individuals.

Thoropass will provide the information in a reasonable time and within one (1) month, at the time of first communication; or when the personal data is first disclosed.

Thoropass does not intend for further processing of personal data other than what it was originally collected for; however, Thoropass will provide the individual with additional information on the purpose for this further processing if Thoropass does further process personal data other than what it was originally collected for.

**Recommendations:** No further recommendations at this time.

## Article 15 Right of Access by the Data Subject

| Fully Compliant | **Evidence:** PT-02 Authority to Process PII (Individual Rights - Access / Amend / Restrict / Object / Delete) |
|---|---|

**Regulation:**

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

**Observations/Findings:**
Thoropass provides individuals the right to obtain confirmation of any personal data Thoropass may process on them. Thoropass provides access to the personal data along with the following information:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients (or categories of recipients) to whom the personal data has been (or will be) disclosed especially those recipients in third countries (or international organizations);
- The estimated period of time the personal data will be stored, where possible, or the criteria used to determine the time period;
- The existences of the right to request rectification, erasure of personal data, restriction of processing of personal data concerning the individual, or object to processing;
- The right to lodge a complaint with a supervisory authority;
- Where the personal data is not collected from the individual, any available information as to the source;
- The existence of automated decision-making (including profiling) and any meaningful information about the logic involved as well as any significant envisaged consequences of the individual for such processing; and
- Where personal data is transferred to a third country (or international organization), the individual has the right to be informed of the appropriate safeguards related to the transfer.

Thoropass provides a copy of personal data as long as it doesn't adversely affect the rights or freedoms of another individual. *Note: Thoropass has not had any access requests from individuals over the last twelve (12) months.*

**Recommendations:** No further recommendations at this time.

## Article 16 Right to Rectification

| Fully Compliant | **Evidence:** PT-02 Authority to Process PII (Individual Rights - Access / Amend / Restrict / Object / Delete) |
|---|---|

**Regulation:**
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

**Observations/Findings:**
Thoropass permits individuals to update or correct their personal data. Thoropass doesn't share personal data with third-parties; however, Thoropass would provide updates or corrections to third parties if ever disclosed. *Note: Thoropass has not had any correction requests from individuals over the last twelve (12) months.*

**Recommendations:** No further recommendations at this time.

## Article 17 Right to Erasure (Right to be Forgotten)

| Fully Compliant | **Evidence:** PT-02 Authority to Process PII (Individual Rights - Access / Amend / Restrict / Object / Delete) |
|---|---|

**Regulation:**

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defense of legal claims.

**Observations/Findings:**

Thoropass provides for the right of individuals to request erasure of their personal data. Thoropass erases personal data without undue delay where one of the following applies:

- The personal data is no longer necessary in relation to the purposes for which the personal data was collected/processed;
- The individual withdrawals consent on which the processing is based and there is no other legal ground for processing;
- The individual objects to processing and there is no overriding legitimate grounds for the processing or the individual objects to the processing of personal data found to have no compelling legitimate grounds for processing;
- The personal data has been unlawfully processed;
- The personal data has to be erased for compliance with legal obligations; or
- The personal data has been collected in relation to the offer of information society services.

Thoropass informs other organizations of the request to erase personal data.

Thoropass informs individuals of any denial of request to erase personal data under the following reasons:

- For exercising the right of freedom of expression and information;
- For compliance with legal obligations;

- For reasons of public interest in the area of public health;
- For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in so far as the right to erasure is likely to render impossible (or seriously impair) the achievement of the objectives of the processing; or
- For the establishment, exercise, or defense of legal claims.

*Note: Thoropass has not had any deletion requests from individuals over the last twelve (12) months.*

**Recommendations:** No further recommendations at this time.

## Article 18 Right to Restriction of Processing

| Fully Compliant | **Evidence:** PT-02 Authority to Process PII (Individual Rights - Access / Amend / Restrict / Object / Delete) |
|---|---|

**Regulation:**

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

**Observations/Findings:**

Thoropass provides for the right of an individual to restrict processing of their personal data where one of the following applies:

- The accuracy of the personal data is contested by the individual for a period of time enabling the organization to verify the accuracy of the personal data;
- The processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of its use instead;
- Thoropass no longer needs the personal data for the purposes of the processing, but is required by the individual for the establishment, exercise, or defense of legal claims; or
- The individual has objected to processing on legitimate grounds pending the verification whether the legitimate grounds of Thoropass override those of the individual.

Thoropass only processes personal data where processing has been restricted, except for storage, with individual consent, exercising legal claim, protection of rights of others, or important public interest.

Thoropass informs individuals who have obtained restrictions before the restrictions of processing have been lifted.

*Note: Thoropass has not had any restriction requests from individuals over the last twelve (12) months.*

**Recommendations:** No further recommendations at this time.

## Article 19 Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing

| Fully Compliant | **Evidence:** PT-05 Privacy Notice (Transparency) |
|---|---|

**Regulation:**
The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

**Observations/Findings:**
Thoropass communicates any rectification or erasure of personal data along with restrictions to recipients to whom the personal data was disclosed. Thoropass informs the individual about the rectification upon request. *Note: Thoropass has not had any rectification/erasure requests from individuals or the need to communicate with individuals regarding these types of requests over the last twelve (12) months.*

**Recommendations:** No further recommendations at this time.

## Article 20 Right to Data Portability

| Fully Compliant | **Evidence:** PT-02 Authority to Process PII (Individual Rights - Access / Amend / Restrict / Object / Delete) |
|---|---|

**Regulation:**
The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means.

In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

**Observations/Findings:**
Thoropass provides the right of an individual to receive their personal data in a structured, commonly used, and machine readable format. Thoropass provides for the right to transmit an individual's personal data to another organization without hindrance. An individual may exercise their right to have their personal data transmitted directly to another organization. *Note: Thoropass has not had any request related to the portability of data or any requests to transmit personal data to another organization over the last twelve (12) months.*

**Recommendations:** No further recommendations at this time.

## Article 21 Right to Object

| Fully Compliant | **Evidence:** PT-02 Authority to Process PII (Individual Rights - Access / Amend / |
|---|---|

| | |
|---|---|
| | Restrict / Object / Delete) |

**Regulation:**
The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

**Observations/Findings:**
Thoropass provides for the right of an individual to object to processing of their personal data including processing based on profiling. Thoropass does not perform any profiling activities. Thoropass will not process personal data under an objection unless it can demonstrate a compelling legitimate ground for the processing. Thoropass will not process personal data for marketing purposes if an individual objects. Thoropass brings the right of objection to the attention of an individual upon first communication with the individual. *Note: An individual has the right to object to processing of their personal data unless the processing is necessary for the performance of a task carried out in the public interest.*

*Note: Thoropass has not had objection requests from individuals over the last twelve (12) months.*

**Recommendations:** No further recommendations at this time.

## Article 22 Automated Individual Decision-Making, Including Profiling

| | |
|---|---|
| Not Applicable | **Evidence:** N/A |

**Regulation:**
The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Paragraph 1 shall not apply if the decision:
- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

**Observations/Findings:**
Not applicable. Thoropass does not conduct any automated individual decision-making activities or profiling activities.

**Recommendations:** Not applicable.

## Article 23 Restrictions

| Fully Compliant | **Evidence:** PT-07 Specific Categories of PII (Use / Disclosure Limitations and Restrictions) |
|---|---|

**Regulation:**
Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defense;
- public security;
- the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- the protection of judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- the protection of the data subject or the rights and freedoms of others;
- the enforcement of civil law claims.

In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- the purposes of the processing or categories of processing;
- the categories of personal data;
- the scope of the restrictions introduced;
- the safeguards to prevent abuse or unlawful access or transfer;
- the specification of the controller or categories of controllers;
- the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- the risks to the rights and freedoms of data subjects; and
- the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

**Observations/Findings:**
Thoropass complies with local jurisdictions that may restrict legislative measures and the scope of obligations (or rights) to individuals (and Thoropass) related to compliance with the GDPR.

**Recommendations:** No further recommendations at this time.

# Chapter 4 Controller and Processor

## Article 24 Responsibility of the Controller

| Fully Compliant | **Evidence:** PT-01 Privacy Policy and Procedures |
|---|---|

**Regulation:**
Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity

for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

**Observations/Findings:**
Thoropass's management is committed and takes responsibility for implementing appropriate technical and organizational safeguards to ensure the protection of processing of personal data considering the nature, scope, context, and purpose of processing as well as risks. Thoropass is also committed to demonstrating compliance of personal data processing. Thoropass reviews and updates implemented measures as necessary.

**Recommendations:** No further recommendations at this time.

## Article 25 Data Protection by Design and by Default

| Fully Compliant | **Evidence:** SA-08 Security and Privacy Engineering Principles |
|---|---|

**Regulation:**
Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

**Observations/Findings:**
Thoropass implements appropriate data protection policy and adheres to code of conducts (or certifications).

**Recommendations:** No further recommendations at this time.

## Article 26 Joint Controllers

| Fully Compliant | **Evidence:** PT-01 Privacy Policy and Procedures |
|---|---|

**Regulation:**
Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

**Observations/Findings:**
If Thoropass jointly determines the purpose and means of processing with another joint controller, Thoropass determines respective responsibilities for compliance and responsibilities for the rights of individuals within an agreement. A contact point for individuals is designated. An individual may exercise their rights under GDPR against each of the controllers.

**Recommendations:** No further recommendations at this time.

## Article 27 Representatives of Controllers or Processors Not Established in the Union

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

The obligation laid down in paragraph 1 of this Article shall not apply to:

- processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offenses referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
- a public authority or body.

The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored, are.

The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

**Observations/Findings:**
Not applicable. The EU representation does not apply to Thoropass since processing is considered occasional, does not include (on a large scale) processing of special categories of data or processing of personal data relating to criminal convictions/offenses, and Thoropass's processing of personal data is unlikely to result in a risk to the rights and freedoms of natural persons (taking into account the nature, context, scope, and purposes of processing).

**Recommendations:** Not applicable.

## Article 28 Processor

| Fully Compliant | **Evidence:** PT-01 Privacy Policy and Procedures; Processor Contract |
|---|---|

**Regulation:**
Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

The processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all measures required pursuant to Article 32;
- respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
- assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).
A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

**Observations/Findings:**

Thoropass, as a processor, provides sufficient guarantees to implement appropriate technical and organizational measures ensuring processing meets requirements of the GDPR and ensures individual privacy right protections. Thoropass only engages other sub-processors with specific written authorization of the controller. Thoropass is governed by a contract binding the organization with regards to the controller. The contract stipulates Thoropass must:

- Process personal data only as instructed in writing from the controller including transfers of personal data to third countries or international organizations. Thoropass will inform the controller of legal requirements for processing unless prohibited by law on the grounds of

public interest;
- Ensure persons authorized to process personal data are committed to confidentiality or are under appropriate statutory obligation of confidentiality;
- Takes all measures required to ensure security of processing;
- Respect conditions for engaging another subprocessor;
- Assist the controller in their fulfillment of the controller's obligation to respond to requests for individuals exercising their rights taking into account the nature of processing and the appropriate technical and organizational measures possible;
- Assist controller in ensuring compliance with security of processing, notification of data breaches to supervisory authority, communication of breaches to individuals, data protection impact assessment and prior consultation with the data protection officer;
- Delete or return personal data at the choice of the controller after the end of services unless required by law;
- Make information available to controller necessary to demonstrate compliance with obligations and allow for/contribute to audits including inspections conducted by the controller; and
- Immediately inform the controller, if in Thoropass's opinion, an instruction infringes on the GDPR or other data protection provisions.

**Recommendations:** No further recommendations at this time.

## Article 29 Processing Under the Authority of the Controller or Processor

| Fully Compliant | **Evidence:** PT-01 Privacy Policy and Procedures |
|---|---|

**Regulation:**
The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

**Observations/Findings:**
Thoropass, as a processor, and any person acting under the authority of Thoropass who accesses personal data is prohibited from processing this data except as instructed by the controller or as required by law.

**Recommendations:** No further recommendations at this time.

## Article 30 Records of Processing Activities

| Fully Compliant | **Evidence:** PM-21 Accounting of Disclosures; Record of Processing |
|---|---|

**Regulation:**
Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing

activities carried out on behalf of a controller, containing:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offenses referred to in Article 10.

**Observations/Findings:**
Thoropass has less than 250 individuals and does not carry out any processing resulting in a restriction of rights or freedoms of data subjects, the processing is occasional, or the processing doesn't include any special categories of personal data or processing related to criminal convictions/offenses. This requirement to maintain a record of processing doesn't apply to Thoropass; however, Thoropass (as a processor) and representative (where applicable) maintains a record (in writing or digital form) of all categories of processing activities containing:

- Name and contact details of Thoropass and of each controller on behalf of which Thoropass is acting and where applicable, the controller's (or the processor's) representative, and data protection officer;
- The categories of processing carried out;
- Transfers of personal data to third country (where applicable) including identification of third country and suitable safeguards; and
- General description of technical and organizational security measures, where possible.

The records may be made available to the supervisory authority on request.

**Recommendations:** No further recommendations at this time.

## Article 31 Cooperation with the Supervisory Authority

| Fully Compliant | **Evidence:** PT-01 Privacy Policy and Procedures |
|---|---|

**Regulation:**
The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

**Observations/Findings:**
Thoropass cooperates with a supervisory authority in the performance of their tasks.

**Recommendations:** No further recommendations at this time.

## Article 32 Security of Processing

| Fully Compliant | **Evidence:** CA-01 Assessment, Authorization, and Monitoring Policy and |
|---|---|

| | |
|---|---|
| | Procedures; CA-02 Control Assessments; CP-01 Contingency Planning Policy and Procedures; CP-02 Contingency Plan (BCP/DR); SC-08 Transmission Confidentiality and Integrity |

**Regulation:**
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

**Observations/Findings:**
Thoropass implements appropriate technical and organizational measures to ensure a level of security appropriate to risk to include:

- Encryption of personal data;
- Ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems;
- Ability to restore the availability and access to personal data in a timely manner in the event of an incident; and
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure security of processing.

Thoropass ensures employees (or contractors) under the authority of Thoropass and who have access to personal data will not process the personal data except instructed by Thoropass (or unless required by law).

**Recommendations:** No further recommendations at this time.

## Article 33 Notification of a Personal Data Breach to the Supervisory Authority

| | |
|---|---|
| Fully Compliant | **Evidence:** IR-04 Incident Handling and Reporting; Breach Notification Template |

**Regulation:**
In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification referred to in paragraph 1 shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

**Observations/Findings:**
In the case of a personal data breach, Thoropass (as a processor) notifies the controller without undue delay and no later than seventy-two (72) hours after becoming aware of a breach.

Notifications of personal data breach will enable the supervisory authority to verify Thoropass's compliance with the GDPR and will contain at least the following:

- Describe the nature of the personal data breach including the categories and approximate number of data subjects concerned as well as the categories and approximate numbers of personal data records concerned, if possible;
- Communicate the name and contact details of the data protection officer (or other contact point) where more information can be obtained;
- Describe likely consequences of the personal data breach;
- Describe measures taken (or proposed) by the controller to address the personal data breach including any measures to mitigate possible adverse effects; and
- If it is not possible to provide all the information at the same time, the information will be provided in phases without undue further delays.

**Recommendations:** No further recommendations at this time.

## Article 34 Communication of a Personal Data Breach to the Data Subject

| Fully Compliant | **Evidence:** IR-04 Incident Handling and Reporting; Sample of Breach Notifications |
|---|---|

**Regulation:**
When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

- the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

**Observations/Findings:**
If the personal data breach is likely to result in a high risk to the rights/freedoms of natural persons, Thoropass will notify the controller. Thoropass will assist the controller, as necessary, to communicate the personal data breach to the data subjects without undue delay. The communication with the impacted data subjects is in clear and plain language and covers the information above [See Article 33].

**Recommendations:** No further recommendations at this time.

## Article 35 Data Protection Impact Assessment

Fully Compliant | **Evidence:** RA-08 Privacy Impact Assessments; Privacy Impact Assessment

**Regulation:**
Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offenses referred to in Article 10; or
- a systematic monitoring of a publicly accessible area on a large scale.

The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behavior in several Member States, or may substantially affect the free movement of personal data within the Union.

The assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to

which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

**Observations/Findings:**
Thoropass carries out an assessment of the impact of envisaged processing operations on the protection of personal data where a type of processing uses new technology taking into account the nature, scope, context, and purpose of the processing, which may be likely to result in a high risk of rights/freedoms of individuals. Thoropass seeks the advice of the data protection officer when carrying out data protection impact assessment activities.

The data protection impact assessment contains at least the following:

- A systematic description of the envisaged processing operations and the purposes of the processing to include any legitimate interest pursued as applicable;
- An assessment of the necessity and proportionality of the processing in relations to its purpose;
- An assessment of the rights to the rights/freedoms of individuals; and
- Measures envisaged to address risks including safeguards, security measures, and other mechanisms ensuring the protection of personal data in order to demonstrate compliance with the GDPR taking into account rights and interests of individuals or others concerned.

Thoropass complies with any relevant approved codes of conduct when assessing the impact of processing and when conducting a DPIA.

Thoropass carries out a review of the DPIA (at least annually) or when there is a change in the risk represented by processing operations.

**Recommendations:** No further recommendations at this time.

## Article 36 Prior Consultation

Fully Compliant | **Evidence:** RA-08 Privacy Impact Assessments; Risk Assessment

**Regulation:**
The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

- where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
- the purposes and means of the intended processing;
- the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
- where applicable, the contact details of the data protection officer;
- the data protection impact assessment provided for in Article 35; and

- any other information requested by the supervisory authority.

Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorization from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

**Observations/Findings:**
Thoropass will consult the supervisory authority prior to processing where a data protection impact assessment indicates processing would result in a high risk in the absence of measures taken by Thoropass to mitigate the risk. Thoropass will provide the supervisory authority with:

- Where applicable, the respective responsibilities of Thoropass, joint controllers, and processors involved in the processing or processing within a group of undertakings;
- The purpose and means of the intended processing;
- The measures/safeguards provided to protect the rights/freedoms of data subjects;
- Where applicable, the contact details of the data protection officer;
- The DPIA; and
- Any other information requested by the supervisory authority.

**Recommendations:** No further recommendations at this time.

## Article 37 Designation of the Data Protection Officer

| Fully Compliant | **Evidence:** PM-19 Privacy Program Leadership Role; Data Protection Officer Designation |
|---|---|

**Regulation:**
The controller and the processor shall designate a data protection officer in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offenses referred to in Article 10.

A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organizational structure and size.

In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39.

The data protection officer may be a staff member of the controller or processor, or fulfill the tasks on the basis of a service contract.

The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

**Observations/Findings:**
Thoropass designates a data protection officer; however, Thoropass does not process personal data as a public authority/body, requiring regular/systematic monitoring of data subjects on a large scale, or process on a large scale of special categories or personal data relating to criminal convictions/offenses.

The data protection officer is designated based on professional qualities and expert knowledge of data protection law, practices, and ability to fulfill tasks. The data protection officer is Jay Trinckes. Thoropass publishes the contact details of the data protection officer and communicates these details to the supervisory authority as applicable.

**Recommendations:** No further recommendations at this time.

## Article 38 Position of the Data Protection Officer

Fully Compliant | **Evidence:** PM-19 Privacy Program Leadership Role

**Regulation:**
The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

The data protection officer may fulfill other tasks and duties. 2The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

**Observations/Findings:**
The data protection officer is involved in all issues related to the protection of personal data. Thoropass supports the data protection officer in performing their tasks by providing necessary resources to carry out those tasks and any access to personal data or operations as well as assisting in maintaining the data protection officer's expert knowledge. Thoropass ensures the data protection officer does not receive any instructions regarding the exercise of those tasks. The data protection officer can not be dismissed or penalized by Thoropass for performing their tasks. The data protection officer reports directly to the highest management level of the organization. Data subjects may contact the data protection officer regarding any issues related to processing of their personal data and to exercise their rights under the GDPR. The data protection officer is bound by secrecy and confidentiality in performing their tasks. The data protection officer may fulfill other tasks and assigned duties; however, Thoropass will ensure these tasks/duties do not result in a conflict of interest.

**Recommendations:** No further recommendations at this time.

## Article 39 Tasks of the Data Protection Officer

Fully Compliant | **Evidence:** PM-19 Privacy Program Leadership Role; DPO Job Description

**Regulation:**
The data protection officer shall have at least the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
- to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

**Observations/Findings:**
The data protection officer is assigned the following minimum tasks:

- Inform and advice Thoropass and employees carrying out processing of their obligations to the GDPR regulations to protect data;
- Monitor compliance with the GDPR and other regulations as well as policies of Thoropass related to protecting personal data including assigned responsibilities, awareness training, and related audits;
- Provide advice where requested related to data protection impact assessment and monitor of its performance;
- Cooperate with the supervisory authority; and
- Act as the contact point for the supervisory authority on issues related to processing including any prior consultation as well as consult, where appropriate, with regard to any other matter.

The data protection officer considers risks associated with operations in performance of their duties taking into account nature, scope, context, and purpose of processing.

**Recommendations:** No further recommendations at this time.

## Articles 40 - 43 Code of Conduct/Certifications

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
See Appendix C for additional information.

**Observations/Findings:**
Not applicable. Thoropass is researching and investigating the EuroPrivacy certification framework at this time.

**Recommendations:** Not applicable.

# Chapter 5 Transfers of Personal Data to Third Countries or International Organizations

## Article 44 General Principle for Transfers

| Fully Compliant | **Evidence:** CA-03 Third-Party Agreements; SR - Third Party Risk Management Policy and Procedures |
|---|---|

**Regulation:**
Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

**Observations/Findings:**
Thoropass transfers personal data undergoing (or intended) for processing to a third country (or to an international organization) only if the controller (or processor) complies with the GDPR. This also includes any onward transfers of personal data from a third country to another third country.

**Recommendations:** No further recommendations at this time.

## Article 45 Transfers on the Basis of an Adequacy Decision

| Fully Compliant | **Evidence:** CA-03 Third-Party Agreements; SR - Third Party Risk Management Policy and Procedures |
|---|---|

**Regulation:**
A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.

When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

- the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- the international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organization ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organization. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

The Commission shall, on an ongoing basis, monitor developments in third countries and international organizations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organization no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

The Commission shall enter into consultations with the third country or international organization with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organization in question pursuant to Articles 46 to 49.

The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organizations for which it has decided that an adequate level of protection is or is no longer ensured.

Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

**Observations/Findings:**
Transfers are contingent upon a determination of adequacy by The Commission [of the EU] to ensure adequate levels of protection are in place within the third country.

**Recommendations:** No further recommendations at this time.

## Article 46 Transfers Subject to Appropriate Safeguards

| Fully Compliant | **Evidence:** CA-03 Third-Party Agreements; SR - Third Party Risk Management Policy and Procedures |
|---|---|

**Regulation:**
In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorization from a supervisory authority, by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47;
- standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Subject to the authorization from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or
- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

Authorizations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

**Observations/Findings:**
If The Commission has not determined adequacy of a third country, Thoropass may still transfer personal data to a third country only if the controller (or processor) has provided appropriate safeguards as well as conditions are available to enforce data subject rights and effective legal remedies for data subjects.

The following appropriate safeguards are provided for without requiring authorization by a supervisory authority:

- A legally binding and enforcementable instrument (such as a contract) between public authorities or bodies;
- Binding corporate rules (according to GDPR Article 47);
- Standard data protection clauses adopted by The Commission according to GDPR Article 93(2);
- Standard data protection clause adopted by a supervisory authority and approved by The Commission referred to in GDPR Article 93(2);
- An approved code of conduct pursuant to GDPR Article 40 along with a binding and enforceable commitment of the controller (or processor) in the third country to apply appropriate safeguards including regards to data subject's rights; or
- An approved certification mechanism pursuant to GDPR Article 42 along with a binding and enforceable commitment of the controller (or processor) in the third country to apply appropriate safeguards including regards to data subject's rights.

The following appropriate safeguards are provided for, but are subject to authorization by a supervisory authority:

- Contractual clauses between the controller (or processor) and the controller, processor, or the recipient of the personal data in the third country; or
- Provisions inserted into administrative arrangements between public authorities (or bodies) including enforceable and effective data subject rights.

**Recommendations:** No further recommendations at this time.

## Article 47 Binding Corporate Rules

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
See Appendix C for additional information.

**Observations/Findings:**
Supervisory authorities must approve binding corporate rules according to a consistent mechanism set out in Article 63. This article is not applicable to Thoropass.

**Recommendations:** Not applicable.

## Article 48 Transfers or Disclosures Not Authorized by Union Law

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

**Observations/Findings:**
Any judgment of a court (or tribunal) and any decision of an administrative authority of a third country requiring a controller (or processor) to transfer/disclose personal data may only be recognized (or enforceable) in any manner if based on an international agreement (a mutual legal assistance treaty) in force between the requesting third country and the Union (or a Member State), without prejudice to other grounds for transfer pursuant to GDPR. This article is not applicable to Thoropass.

**Recommendations:** Not applicable.

## Article 49 Derogations for Specific Situations

| Fully Compliant | **Evidence:** CA-03 Third-Party Agreements; SR - Third Party Risk Management Policy and Procedures; Determination of Adequacy |
|---|---|

**Regulation:**
In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognized in Union law or in the law of the Member State to which the controller is subject.

In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organization. Member States shall notify such provisions to the Commission.

The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

**Observations/Findings:**
In the absence of an adequacy decision or appropriate safeguards (including binding corporate rules), Thoropass may transfer personal data to a third country only if one of the following conditions apply:

- The data subject explicitly consented to the proposed transfer after being given information of possible risks to the transfer due to the lack of adequacy/safeguards;
  *Note: This does not apply to public authorities in the exercise of their public powers.*
- The transfer is necessary to perform a contract between the data subject and the controller or as part of pre-contractual measures taken at the request of the data subject;
  *Note: This does not apply to public authorities in the exercise of their public powers;*
- The transfer is necessary for the performance/conclusion of a contract in the data subject's interest between the controller and another person;
  *Note: This does not apply to public authorities in the exercise of their public powers;*
- The transfer is necessary for important reasons of public interest;
  *Note: Public interest must be recognized by Union law (or in the law of the Member State) to which the controller is subject. The Union (or Member State) may set limits on transfer of special categories of personal data when it comes to the public interest;*
- The transfer is necessary for the establishment, exercise, or defense of legal claims;
- The transfer is necessary in order to protect the vital interest of the data subject (or other person) where the data subject is physically/legally incapable of giving consent; or
- The transfer is made from a register, which according to Union (or Member State law) is intended to provide information to the public and which is open to consultation either by the public or by any person demonstrating a legitimate interest, but only to the extent conditions are laid down by Union (or Member State law) for consultation are fulfilled in the particular case.
  *Note: Transfer related to register will not involve the entirety of the personal data (or entire categories of personal data) contained in the register. If the register is intended for consultation by persons having a legitimate interest, the transfer will be made only at the request of those persons (or if they are to be the recipients).*

In the absence of an adequacy decision or appropriate safeguards (including binding corporate rules and none of the above applies, Thoropass may transfer personal data to a third country only if one of these additional conditions apply:

- The transfer is not repetitive;
- Concerns only a limited number of data subjects;
- Is necessary for the purposes of compelling legitimate interests pursued by Thoropass, which are not overridden by the interests of rights/freedoms of the data subject; and
- Thoropass has assessed all the circumstances surrounding the data transfer and has, on the basis of the assessment, provided suitable safeguards with regard to the protection of personal data.

Thoropass must inform the supervisory authority of the transfer. Thoropass will provide the necessary information and inform the data subject of the transfer with the compelling legitimate interests pursued. Thoropass (as a processor) documents the assessment performed on the determination of a transfer as well as the suitable safeguards in place and referenced above.

**Recommendations:** No further recommendations at this time.

### Article 50 International Cooperation for the Protection of Personal Data

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
In relation to third countries and international organizations, the Commission and supervisory authorities shall take appropriate steps to:

- develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
- provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
- promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

**Observations/Findings:**
The Commission and supervisory authorities will take steps to develop international cooperation mechanisms to facilitate the effective enforcement of the GDPR through notification, complaint referral, investigative assistance, and information exchange subject to safeguards over the protection of personal data and fundamental rights/freedoms. This article is not applicable to Thoropass.

**Recommendations:** Not applicable.

## Chapter 6 Independent Supervisory Authorities

### Articles 51 - 59 Supervisory Authorities

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
See Appendix C for additional information.

**Observations/Findings:**
Not applicable. These are articles related to supervisory authority obligations.

**Recommendations:** Not applicable.

## Chapter 7 Cooperation and Consistency

### Articles 60 - 76 Cooperation and Consistency

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
See Appendix C for additional information.

**Observations/Findings:**
Not applicable. These are articles related to cooperation and consistency between supervisory authorities.

| |
|---|
| **Recommendations:** Not applicable. |

# Chapter 8 Remedies, Liability, and Penalties

## Articles 77 - 84 Remedies, Liability, and Penalties

| | |
|---|---|
| Not Applicable | **Evidence:** N/A |
| **Regulation:**<br>See Appendix C for additional information. | |
| **Observations/Findings:**<br>Not applicable. These are articles related to remedies, liabilities, and penalties. | |
| **Recommendations:** Not applicable. | |

# Chapter 9 Provisions Relating to Specific Processing Situations

## Articles 85 - 88 Specific Processing

| | |
|---|---|
| Not Applicable | **Evidence:** N/A |
| **Regulation:**<br>See Appendix C for additional information. | |
| **Observations/Findings:**<br>Not applicable. These are articles related to specific processing not relevant to Thoropass. | |
| **Recommendations:** Not applicable. | |

## Article 89 Safeguards and Derogations Relating to Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes

| | |
|---|---|
| Fully Compliant | **Evidence:** PT-07 Specific Categories of PII (Use / Disclosure Limitations and Restrictions); SI-03 Malware and Endpoint Protection |
| **Regulation:**<br>Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. 4Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.<br><br>Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State | |

law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of those purposes.

Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of those purposes.

Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

**Observations/Findings:**
Thoropass does not process personal data for archiving purposes in the public interest, scientific, or historical research purposes, or statistical purposes. Thoropass ensures technical and organizational measures are in place for safeguards to include the principle of data minimization. Safeguards include encryption, where applicable.

**Recommendations:** No further recommendations at this time.

### Articles 90 - 91 Specific Processing

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
See Appendix C for additional information.

**Observations/Findings:**
Not applicable. These are articles related to specific processing not relevant to Thoropass.

**Recommendations:** Not applicable.

## Chapter 10 Delegated Acts and Implementing Acts

### Articles 92 - 93 Delegated Acts and Implementing Acts

| Not Applicable | **Evidence:** N/A |
|---|---|

**Regulation:**
See Appendix C for additional information.

**Observations/Findings:**
Not applicable. These are articles related to delegated acts and implementing a

**Recommendations:** Not applicable.

# Chapter 11 Final Provisions

## Articles 94 - 99 Final Provisions

| Not Applicable | **Evidence:** N/A |
|---|---|
| **Regulation:**<br>See Appendix C for additional information. | |
| **Observations/Findings:**<br>Not applicable. These are articles related to final provisions of the GDPR. | |
| **Recommendations:** Not applicable. | |

# Appendices

## Appendix A - Project Team

The following were the assigned Project Team Members during this assessment:

| **Thoropass** | |
|---|---|
| **Role** | **Team Member** |
| Co-Founder/COO (Executive Management) | Eva Pittas |
| VP, Engineering (Approver) | Scott Schlegel |
| Data Protection Officer/CISO (Assessor) | Jay Trinckes |

## Appendix B - List of Evidence Reviewed

The following was a list of documents reviewed during this assessment:

1. Access Requests
2. Assessment, Authorization, and Monitoring Policy
3. Breach Notification Template
4. Consent Evidence
5. Contingency Planning Policy
6. Data Protection Officer Designation
7. Data Protection Officer Job Description
8. Determination of Adequacy
9. Incident Handling and Reporting Policy
10. Information Security Program Management Policy
11. Privacy Impact Assessment
12. Privacy Notice

13. Privacy Policy
14. Processor Contract
15. Record of Processing
16. Risk Assessment Policy
17. Sample of Breach Notifications
18. System Development Life Cycle (SDLC) Policy
19. System Integrity Policy
20. System Protection Policy
21. Third Party Risk management Policy and Procedures

# Appendix C - Selected Article Regulations

**Article 1 Subject-matter and Objectives**
This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

**Article 2 Material Scope**
This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

This Regulation does not apply to the processing of personal data:
- in the course of an activity which falls outside the scope of Union law;
- by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
- by a natural person in the course of a purely personal or household activity;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

**Article 3 Territorial Scope**
This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behavior as far as their behavior takes place within the Union.

This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

**Article 4 Definitions**
For the purposes of this Regulation:
- ‘personal data’ means 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;
- ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;
- ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
- ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
- ‘controller’ means 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’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;
- ‘consent’ of the data subject means 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’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- ‘main establishment’ means: as regards 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; as regards 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 take place to the extent that the processor is subject to specific obligations under this Regulation;
- ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
- ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;
- ‘binding corporate rules’ means 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’ means an independent public authority which is established by a Member State pursuant to Article 51;
- ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because: the controller or processor is established on the territory of the Member State of that supervisory authority; data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or a complaint has been lodged with that supervisory authority;
- ‘cross-border processing’ means either: 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 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.
- ‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;

- ‘international organization’ means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

**Article 40 Codes of Conduct**

The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

- fair and transparent processing;
- the legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymization of personal data;
- the information provided to the public and to data subjects;
- the exercise of the rights of data subjects;
- the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
- the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
- the transfer of personal data to third countries or international organizations; or
- out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organizations under the terms referred to in point (e) of Article 46(2). 2Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

### Article 41 Monitoring of Approved Codes of Conduct

Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

- demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;
- established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
- established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

The competent supervisory authority shall submit the draft requirements for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the requirements for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

This Article shall not apply to processing carried out by public authorities and bodies.

### Article 42 Certification

The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organizations under the terms referred to in point (f) of Article 46(2). 2Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

The certification shall be voluntary and available via a process that is transparent.

A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant criteria continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the criteria for the certification are not or are no longer met.

The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

**Article 43 Certification Bodies**

Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

- the supervisory authority which is competent pursuant to Article 55 or 56;
- the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council[1] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

- demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
- undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;
- established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of requirements approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. 2In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board.

Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognize those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

**Article 47 Binding Corporate Rules**

The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

- are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
- expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
- fulfill the requirements laid down in paragraph 2.

The binding corporate rules referred to in paragraph 1 shall specify at least:

- the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- their legally binding nature, both internally and externally;
- the application of the general data protection principles, in particular purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
- the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;
- how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;
- the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
- the complaint procedures;
- the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;
- the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
- the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);
- the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- the appropriate data protection training to personnel having permanent or regular access to personal data.

The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

**Article 51 Supervisory Authority**

Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).

Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

### Article 52 Independence

Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

### Article 53 General Conditions for the Members of the Supervisory Authority

Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

- their parliament;
- their government;
- their head of State; or
- an independent body entrusted with the appointment under Member State law.

Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfills the conditions required for the performance of the duties.

### Article 54 Rules on the Establishment of the Supervisory Authority

Each Member State shall provide by law for all of the following:

- the establishment of each supervisory authority;
- the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;
- the rules and procedures for the appointment of the member or members of each supervisory authority;
- the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
- whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;
- the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which

has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

### Article 55 Competence

Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

### Article 56 Competence of the Lead Supervisory Authority

Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

### Article 57 Tasks

Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

- monitor and enforce the application of this Regulation;
- promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
- advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
- promote the awareness of controllers and processors of their obligations under this Regulation;
- upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
- handle complaints lodged by a data subject, or by a body, organization or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
- cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
- conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
- monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
- establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
- give advice on the processing operations referred to in Article 36(2);

- encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
- encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
- where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
- draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
- conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
- authorize contractual clauses and provisions referred to in Article 46(3);
- approve binding corporate rules pursuant to Article 47;
- contribute to the activities of the Board;
- keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
- fulfill any other tasks related to the protection of personal data.

Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

**Article 58 Powers**

Each supervisory authority shall have all of the following investigative powers:

- to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- to carry out investigations in the form of data protection audits;
- to carry out a review on certifications issued pursuant to Article 42(7);
- to notify the controller or the processor of an alleged infringement of this Regulation;
- to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Each supervisory authority shall have all of the following corrective powers:

- to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- to order the controller to communicate a personal data breach to the data subject;
- to impose a temporary or definitive limitation including a ban on processing;
- to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
- to order the suspension of data flows to a recipient in a third country or to an international organization.

Each supervisory authority shall have all of the following authorization and advisory powers:

- to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

- to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
- to authorize processing referred to in Article 36(5), if the law of the Member State requires such prior authorization;
- to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
- to accredit certification bodies pursuant to Article 43
- to issue certifications and approve criteria of certification in accordance with Article 42(5);
- to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
- to authorize contractual clauses referred to in point (a) of Article 46(3);
- to authorize administrative arrangements referred to in point (b) of Article 46(3);
- to approve binding corporate rules pursuant to Article 47.

The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

### Article 59 Activity Reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

### Article 60 Cooperation Between the Lead Supervisory Authority and the Other Supervisory Authorities Concerned

The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavor to reach consensus. 2The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. 2That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. 2The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardized format.

**Article 61 Mutual Assistance**

Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

The requested supervisory authority shall not refuse to comply with the request unless:

- it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
- compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. 2The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardized format.

Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance.

Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). 2In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardized format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

### Article 62 Joint Operations of Supervisory Authorities

The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. 2In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

### Article 63 Consistency Mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

### Article 64 Opinion of the Board

The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. 2To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

- aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);
- concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;
- aims to approve the requirements for accreditation of a body pursuant to Article 41(3), of a certification body pursuant to Article 43(3) or the criteria for certification referred to in Article 42(5);
- aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);
- aims to authorize contractual clauses referred to in point (a) of Article 46(3); or
- aims to approve binding corporate rules within the meaning of Article 47.

Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter.

Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardized format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

The Chair of the Board shall, without undue, delay inform by electronic means:

- the members of the Board and the Commission of any relevant information which has been communicated to it using a standardized format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and
- the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

The competent supervisory authority referred to in paragraph 1 shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

The competent supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardized format.

Where the competent supervisory authority referred to in paragraph 1 informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

**Article 65 Dispute Resolution by the Board**

In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

- where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;
- where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;
- where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. 2It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and

shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

### Article 66 Urgency Procedure

In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

### Article 67 Exchange of Information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardized format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

### Article 68 European Data Protection Board

The European Data Protection Board (the ‘Board’) is hereby established as a body of the Union and shall have legal personality. The Board shall be represented by its Chair.

The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State’s law.

The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

### Article 69 Independence

The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

Without prejudice to requests by the Commission referred to in Article 70(1) and (2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

### Article 70 Tasks of the Board

The Board shall ensure the consistent application of this Regulation. 2To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

- monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;
- advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

- advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;
- issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);
- examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;
- issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);
- issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;
- issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).
- issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;
- issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);
- draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;
- review the practical application of the guidelines, recommendations and best practices;
- issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);
- encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;
- approve the criteria of certification pursuant to Article 42(5) and maintain a public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8) and of the certified controllers or processors established in third countries pursuant to Article 42(7);
- approve the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies referred to in Article 43;
- provide the Commission with an opinion on the certification requirements referred to in Article 43(8);
- provide the Commission with an opinion on the icons referred to in Article 12(7);
- provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organization no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organization.
- issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;
- promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;
- promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organizations;
- promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.
- issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and
- maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. 2The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

### Article 71 Reports

The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organizations. 2The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

### Article 72 Procedure

The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organize its own operational arrangements.

### Article 73 Chair

The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

### Article 74 Tasks of the Chair

The Chair shall have the following tasks:

- to convene the meetings of the Board and prepare its agenda;
- to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;
- to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

### Article 75 Secretariat

The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

The secretariat shall provide analytical, administrative and logistical support to the Board.

The secretariat shall be responsible in particular for:

- the day-to-day business of the Board;
- communication between the members of the Board, its Chair and the Commission;
- communication with other institutions and the public;
- the use of electronic means for the internal and external communication;
- the translation of relevant information;
- the preparation and follow-up of the meetings of the Board;
- the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

### Article 76 Confidentiality

The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council.

### Article 77 Right to Lodge a Complaint with a Supervisory Authority

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

### Article 78 Right to an Effective Judicial Remedy Against a Supervisory Authority

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

### Article 79 Right to an Effective Judicial Remedy Against a Controller or Processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

### Article 80 Representation of Data Subjects

The data subject shall have the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

Member States may provide that any body, organization or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

### Article 81 Suspension of Proceedings

Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

### Article 82 Right to Compensation and Liability

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

**Article 83 General Conditions for Imposing Administrative Fees**

Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). 2When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- the intentional or negligent character of the infringement;
- any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 and 32;
- any relevant previous infringements by the controller or processor;
- the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- the categories of personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
- the obligations of the certification body pursuant to Articles 42 and 43;
- the obligations of the monitoring body pursuant to Article 41(4).

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- the data subjects' rights pursuant to Articles 12 to 22;
- the transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49;
- any obligations pursuant to Member State law adopted under Chapter IX;
- non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the

- supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

### Article 84 Penalties

Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

### Article 85 processing and Freedom of Expression and Information

Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

### Article 86 Processing and Public Access to Official Documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

### Article 87 Processing of the National Identification Number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

### Article 88 Processing in the Context of Employment

Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

### Article 90 Obligations of Secrecy

Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

### Article 91 Existing Data Protection rules of Churches and Religious Associations

Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfills the conditions laid down in Chapter VI of this Regulation.

### Article 92 Exercise of the Delegation

The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

### Article 93 Committee Procedure

The Commission shall be assisted by a committee. 2That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Where reference is made to this paragraph, Article 8 of Regulation ((EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

### Article 94 Repeal of Directive 95/46/EC

Directive 95/46/EC is repealed with effect from 25 May 2018.
1References to the repealed Directive shall be construed as references to this Regulation. 2References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

### Article 95 Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

### Article 96 Relationship with Previously Concluded Agreements

International agreements involving the transfer of personal data to third countries or international organizations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

### Article 97 Commission Reports

By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. 2The reports shall be made public.

In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

- Chapter V on the transfer of personal data to third countries or international organizations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;
- Chapter VII on cooperation and consistency.

For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

### Article 98 Review of Other Union Legal Acts on Data Protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

### Article 99 Entry into Force and Application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 25 May 2018.