

Internal and Confidential

Netradyne Personal Data Protection Policy

V2.5

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDPRIVACY2021001 |
| **Document Name** | Netradyne Personal Data Protection Policy |
| **Document Status** | Released |
| **Document Initial Release Date** | 01-MAR-2021 |
| **Document Author** | Shivesh Ranjan |
| **Document Content Contributors** | Michael Campos, Kristi Griffith, Shivesh Ranjan |
| **Document Signatory** | Michael Campos<michael.campos@Netradyne.com > |
| **Document Owner** | Michael Campos<michael.campos@Netradyne.com > |
| **Document Version** | V2.5 |
| **Information Classification** | Internal & Confidential |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 01-MAR-2021 | Original issue | Consultant (Kumar) |
| V2.0 | 11-OCT-2021 | Review and clarify applicability to European Union & UK | Michael Campos & Kristi Griffith |
| V2.1 | 22-FEB-2022 | Updated Privacy Governance model | Michael Campos |
| V2.2 | 21-APR-2023 | Updated Implementation & Accountability fields to Document Control | Michael Campos |
| V2.3 | 15-FEB-2023 | Updated “Organization and Responsibilities” section. Added additional role for Finance. | Shivesh Ranjan |
| V2.4 | 06-FEB-2024 | Aligned with standard template.  Updated “Organization and Responsibilities” section. Added reference to PHI in sections 2&4; and reference to BAA in section 8 (under Engineering stakeholder). Added link to ND Privacy Policy in 6.4. | Shivesh Ranjan |
| V2.5 | 03-FEB-2025 | No Changes | Shivesh Ranjan |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 01-MAR-2021 | Michael Campos | Data Protection Officer |  |
| 11-OCT-2021 | Michael Campos | Data Protection Officer |  |
| 22-FEB-2022 | Michael Campos | Data Protection Officer |  |
| 21-APR-2023 | Michael Campos | Data Protection Officer |  |
| 15-FEB-2023 | Michael Campos | Data Protection Officer |  |
| 06-FEB-2024 | Michael Campos | Data Protection Officer |  |
| 10-FEB-2025 | Michael Campos | Data Protection Officer |  |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| All Employees | Netradyne |
|  |  |
|  |  |

Table of Contents

[Document Control 1](#_Toc1849142256)

[1 Purpose 4](#_Toc1499160251)

[2 Scope 4](#_Toc1031888098)

[3 Roles and Responsibilities 4](#_Toc2030143896)

[4 Definitions 4](#_Toc413974671)

[5 Basic Principles Regarding Personal Data Processing 5](#_Toc242247524)

[5.1 Lawfulness, Fairness and Transparency 6](#_Toc1433183119)

[5.2 Purpose Limitation 6](#_Toc612945413)

[5.3 Data Minimization 6](#_Toc1209781788)

[5.4 Accuracy 6](#_Toc81361618)

[5.5 Storage Period Limitation 6](#_Toc1224018269)

[5.6 Integrity and confidentiality 6](#_Toc159683411)

[5.7 Accountability 6](#_Toc1222573364)

[6 Building Data Protection in Business Activities 6](#_Toc923152153)

[6.1 Notification to Data Subjects 6](#_Toc191179431)

[6.2 Data Subject’s Choice and Consent 6](#_Toc66206306)

[6.3 Collection 7](#_Toc607333298)

[6.4 Use, Retention, and Disposal 7](#_Toc2119108872)

[6.5 Disclosure to Third Parties 7](#_Toc1358197121)

[6.6 Cross-border Transfer of Personal Data 7](#_Toc213623692)

[6.7 Rights of Access by Data Subjects 7](#_Toc863102314)

[6.8 Data Portability 7](#_Toc1109614352)

[6.9 Right to be Forgotten 7](#_Toc2116079012)

[7 Fair Processing Guidelines 8](#_Toc335807091)

[7.1 Notices to Data Subjects 8](#_Toc2032857723)

[7.2 Obtaining Consents 8](#_Toc639968718)

[8 Organization and Responsibilities 8](#_Toc1965867476)

[9 Guidelines for Establishing the Lead Supervisory Authority 11](#_Toc325482275)

[9.1 Necessity to Establish the Lead Supervisory Authority 11](#_Toc1217413577)

[9.2 Main Establishment and the Lead Supervisory Authority 12](#_Toc1882146323)

[9.2.1 Main Establishment for the DPO 12](#_Toc1670792533)

[9.2.2 Main Establishment for the Data Processor 12](#_Toc309899393)

[9.2.3 Main Establishment for Non-EU Companies for DPOs and Processors 12](#_Toc167281080)

[10 Response to Personal Data Breach Incidents 12](#_Toc482108344)

[11 Audit and Accountability 12](#_Toc580203500)

[12 Conflicts of Law 12](#_Toc1328225242)

[13 Managing records kept on the basis of this document 12](#_Toc162992394)

[14 Validity and document management 13](#_Toc1018947185)

# Purpose

Netradyne, hereinafter referred to as the “Company”, strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Company operates. This Policy sets forth the basic principles by which the Company processes the Personal Data of consumers, customers, suppliers, business partners, employees, and other individuals, and indicates the responsibilities of its business departments and employees while processing Personal Data.

# Scope

This document applies to all NETRADYNE activities, departments, and divisions processing and/or utilizing personal data (including personal health data (PHI)) of Netradyne’s consumers, customers, suppliers, business partners, employees, and other individuals. The users of this document are all employees, permanent or temporary, and all contractors working on behalf of the Company.

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | Privacy |
| Reviewers/Stakeholders | Legal, InfoSec, Engineering, HR, Finance, Sales, Marketing |
| Approvers | DPO |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# Definitions

The following definitions of terms used in this document are drawn from Article 4 of EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC).

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

**Sensitive Personal Data:** Personal Data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those Personal Data include Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.

**Data Controller** The natural or legal person, public authority, agency, or any other body, which alone or jointly with others, determines the purposes and means of the processing of Personal Data.

**Data Processor**: A natural or legal person, public authority, agency, or any other body which processes Personal Data on behalf of a Data Controller.

**Processing**: An 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 of the data.

**Anonymization:** Irreversibly de-identifying Personal Data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The Personal Data processing principles do not apply to anonymized data as it is no longer Personal Data.

**Pseudonymization:** 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. Pseudonymization reduces, but does not completely eliminate, the ability to link Personal Data to a data subject. Because pseudonymized data is still Personal Data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

**Cross-border processing of Personal Data:** 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 and/or the UK; 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 and/or the UK;

**Supervisory Authority:** An independent public authority which is established by a Member State or the UK pursuant to Article 51 of the EU GDPR;

**Lead supervisory authority:** The supervisory authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her Personal Data; it is responsible, among others, for receiving the data breach notifications, to be notified on risky processing activity and will have full authority as regards to its duties to ensure compliance with the provisions of the EU GDPR;

Each “**local supervisory authority**” will still maintain in its own territory and will monitor any local data processing that affects data subjects or that is carried out by a Union or non-Union controller or processor when their processing targets data subjects residing on its territory. Their tasks and powers include conducting investigations and applying administrative measures and fines, promoting public awareness of the risks, rules, security, and rights in relation to the processing of Personal Data, as well as obtaining access to any premises of the controller and the processor, including any data processing equipment and means.

**“Main establishment as regards a controller”** with establishments in more than one Member State and/or the UK, 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;

**“Main establishment as regards a processor”** with establishments in more than one Member State and/or the UK, 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;

**Group Undertaking:** Any holding company together with its subsidiary.

For avoidance of doubt, personal health information (PHI) would be treated as ‘Sensitive Personal Data’.

# Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for handling Personal Data. Article 5(2) of the GDPR stipulates that “*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*.”. Netradyne will employ adequate organizational, physical, and technical safeguards that are commensurate with the risks and in accordance with applicable laws to protect personal data (including PHI).

Lawfulness, Fairness and Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose Limitation

Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data Minimization

Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The Company must apply anonymization or pseudonymization to Personal Data, if possible, to reduce the risks to the data subjects concerned.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date; reasonable steps 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 in a timely manner.

Storage Period Limitation

Personal Data must be kept for no longer than is necessary for the purposes for which the Personal Data are processed.

Integrity and confidentiality

Considering the state of technology and other available security measures, the implementation cost, and likelihood and severity of Personal Data risks, the Company must use appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of Personal Data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

Accountability

Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

# Building Data Protection in Business Activities

In order to demonstrate compliance with the principles of data protection, the Company should build data protection into its business activities.

Notification to Data Subjects

(See the Fair Processing Guidelines in section 6 of this document.)

Data Subject’s Choice and Consent

(See the Fair Processing Guidelines in section 6 of this document.)

Collection

The Company must strive to collect the least amount of Personal Data possible. If Personal Data is collected from a third party, DPO must ensure that the Personal Data is collected lawfully.

Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of Personal Data must be consistent with the information contained in the [Privacy Notice](https://www.netradyne.com/privacy-policy). Customer specific data retention periods may be specified in the customer contract to suit customers’ requirements and prevailing regulatory obligations. The Company must maintain the accuracy, integrity, confidentiality, and relevance of Personal Data based on the processing purpose. Adequate security mechanisms designed to protect Personal Data must be used to prevent Personal Data from being stolen, misused, or abused, and prevent Personal Data breaches. IT Stakeholder is responsible for compliance with the requirements listed in this section.

Disclosure to Third Parties

Whenever the Company uses a third-party supplier or business partner to process Personal Data on its behalf, the legal/contracts team will consult with appropriate Privacy Stakeholders and the DPO will review to ensure that this processor will provide security measures to safeguard Personal Data that are appropriate to the associated risks.

The Company must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process Personal Data to carry out its contractual obligations towards the Company or upon the instructions of the Company and not for any other purposes. When the Company processes Personal Data jointly with an independent third party, the Company must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement.

Cross-border Transfer of Personal Data

Before transferring Personal Data out of the European Economic Area (EEA) or the UK adequate safeguards must be used including the signing of a Data Transfer Agreement, as required by the Union and, if required, authorization from the relevant Data Protection Authority must be obtained. The entity receiving the Personal Data must comply with the principles of Personal Data processing set forth in this policy.

Rights of Access by Data Subjects

When acting as a data controller, DPO is responsible to provide data subjects with a reasonable access mechanism to enable them to access their Personal Data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure. DPO is responsible to ensure that such requests are processed within one month, are not excessive and do not affect the rights of Personal Data from other individuals.

Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free. DPO is responsible to ensure that such requests are processed within one month, are not excessive and do not affect the rights to Personal Data of other individuals.

Right to be Forgotten

Upon request, Data Subjects have the right to obtain from the Company the erasure of its Personal Data. When the Company is acting as a Controller, DPO must take necessary actions (including technical measures) to inform the third parties who use or process that data to comply with the request.

# Fair Processing Guidelines

Personal Data must only be processed when explicitly authorised by DPO.

The Company must decide whether to perform the Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines.

Notices to Data Subjects

At the time of collection or before collecting Personal Data for any kind of processing activities including but not limited to selling products, services, or marketing activities, DPO is responsible to properly inform data subjects of the following: the types of Personal Data collected, the purposes of the processing, processing methods, the data subjects’ rights with respect to their Personal Data, the retention period, potential international data transfers, information on the data controller, DPO, lawful grounds, if data will be shared with third parties and the Company’s security measures to protect Personal Data. This information is provided through the Privacy Notice.

Where Personal Data is being shared with a third party, DPO must ensure that data subjects have been notified of this through a Privacy Notice.

Where Personal Data is being transferred to a third country according to Cross Border Data Transfer Policy, the Privacy Notice should reflect this and clearly state to where, and to which entity Personal Data is being transferred.

Where sensitive Personal Data is being collected, the DPO must make sure that the Privacy Notice explicitly states the purpose for which this sensitive Personal Data is being collected.

Obtaining Consents

Whenever Personal Data processing is based on the data subject's consent, or other lawful grounds, DPO is responsible for retaining a record of such consent. DPO is responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

Where collection of Personal Data relates to a child under the age of 16, DPO must ensure that parental consent is given prior to the collection using the Parental Consent Form.

When requests to correct, amend or destroy Personal Data records, DPO must ensure that these requests are handled within a reasonable time frame. DPO must also record the requests and keep a log of these.

Personal Data must only be processed for the purpose for which they were originally collected. In the event that the Company wants to process collected Personal Data for another purpose that is incompatible with the original purposes (see Art. 6 (4) GDPR), the Company must seek the consent of its data subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s). The DPO is responsible for complying with the rules in this paragraph.

Now and in the future, DPO must ensure that collection methods are compliant with relevant law, good practices, and industry standards.

DPO is responsible for creating and maintaining a Register of the Privacy Notices.

# Organization and Responsibilities

The responsibility for ensuring appropriate Personal Data processing lies with everyone who works for or with the Company and has access to Personal Data processed by the Company.

Netradyne uses a Hub and Spokes model to operationalize its Privacy Governance Framework. The model consists of one Hub (Privacy Team) providing centralized leadership to the privacy program, and multiple spokes with a Privacy Stakeholder in each corporate function who shares accountability under leadership of the Hub. All identified participants together make up the Privacy Council.

A diagram of a company's company

Description automatically generated

The key areas of responsibilities for processing Personal Data lie with the following organisational roles:

**The CEO or CTO** makes decisions about and approves the Company’s general strategies on Personal Data protection.

The **Privacy Team, including the Data Protection Officer (DPO)** is responsible for the development and promotion of end-to-end Personal Data protection policies, as defined in DPO Job Description; and assists business departments in achieving their Personal Data Protection goals, monitors and analyses Personal Data laws and changes to regulations, and assists existing and prospective customers with privacy related issues.

The Privacy Team is responsible for managing the Personal Data protection program; developing compliance requirements in consultation with the Privacy Stakeholders;

The **Legal stakeholder** is responsible for:

* During contracting, Legal stakeholder identifies legal risks associated with certain terms and seeks advice of DPO and/or outside counsel as required and determines whether negotiated terms are acceptable to the company and relevant stakeholders, in consultation with stakeholders and/or CEO, as required.
* Weighs inputs from Privacy, InfoSec, and Legal and negotiates acceptable contractual terms in consultation with stakeholders.
* Passing on Personal Data protection responsibilities to suppliers and improving suppliers' awareness levels of Personal Data protection as well as flow down Personal Data requirements to any third party or supplier they are using. Where required by law, Contracts must ensure that the Company reserves a right to audit suppliers.
* Attestations (must be from Legal)

Legal stakeholder advises as to whether the identified legal risks associated with certain decisions are acceptable to the company, in consultation with the CEO.

The **InfoSec stakeholder,** is responsible for:

* Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
* Performing regular checks and scans to ensure security hardware and software is functioning properly.
* Improving employees' awareness of information security and data protection guidelines through periodic awareness campaigns.

The **Engineering stakeholder** is responsible for:

* Ensuring all Personal Data handling in cloud production systems complies with company privacy policies and contractual obligations (including customer specific- Data Retention Policy (DRP), Data Usage Policy (DUP), Business Associate Agreement (BAA)).
* Implementing data retention and data usage policies; monitoring and reporting changes that could materially change stated data minimization targets
* Ensuring all Personal Data handling for perceptual engine development, including machine learning datasets, complies with company privacy policies.
* Initiating new Data Privacy Impact Assessments when required.
* Periodically conducting data reviews to identify Personal Data that can be deleted from machine learning datasets.

The **Marketing stakeholder**, is responsible for:

* Approving any data protection statements attached to communications such as emails and letters.
* Addressing any data protection queries from journalists or media outlets like newspapers.
* Where necessary, working with the DPO to ensure marketing initiatives abide by data protection principles. Managing deletion requests related to marketing campaigns.

The **Sales and Customer Success stakeholder** is responsible for ensuring that Personal Data associated with prospective, current, and former customers is handled in compliance with company privacy policies.

The **Product stakeholder** is responsible for:

* Ensuring that Privacy considerations are incorporated into the earliest stages of Product development.
* Weighing company interests in privacy decisions.
* Prioritizing technical privacy roadmap items.
* Initiating new Data Privacy Impact Assessments when required.

The **Human Resources stakeholder,** is responsible for:

* End-to-end employee Personal Data protection. It must ensure that employees' Personal Data is processed based on the employer's legitimate business purposes and necessity.

The **Finance stakeholder** is responsible for approving investments and making budgetary allocations for privacy and data security initiatives, as and when required.

The Privacy Council members are listed below:

|  |  |  |
| --- | --- | --- |
| **#** | **Privacy Council** | **Contact** |
|  | **Privacy Team** |  |
| 1 | Data Protection Officer (DPO) | Michael Campos |
| 3 | Privacy Manager | Shivesh Ranjan |
|  | **Privacy Stakeholders** |  |
| 5 | InfoSec | Saravanan Sankaran |
| 6 | Engineering- Cloud | Vinai Rai  Gaurav Agarwal |
| 7 | Engineering- Analytics | Sreekanth Annapureddy  Hisham Rahman |
| 8 | Marketing | Barrett Young |
| 9 | Customer Success | Heather Engen |
| 10 | Product Management | Pramod Akkarachittor  Arunlal Sreedharan |
| 11 | Human Resources | Pooja Madappa  Kathy Pearson (United States) |
| 12 | Legal | Dev Zaveri |
| 13 | Finance | Tom Schmitt |

# Guidelines for Establishing the Lead Supervisory Authority

Necessity to Establish the Lead Supervisory Authority

Identifying a Lead supervisory authority is only relevant if the Company carries out the cross-border processing of Personal Data.

Cross border of Personal Data is carried out if:

1. *processing of Personal Data is carried out by subsidiaries of the Company which are based in other Member States or the UK;*

*or*

1. *processing of Personal Data which takes place in a single establishment of the Company in the Union, but which substantially affects or is likely to substantially affect data subjects in more than one Member State and/or the UK.*

If the Company only has establishments in one Member State and its processing activities are affecting only data subjects in that Member State than there is no need to establish a lead supervisory authority. The only competent authority will be the Supervisory Authority in the country where Company is lawfully established.

Main Establishment and the Lead Supervisory Authority

### Main Establishment for the DPO

The top management of the Company needs to identify the main establishment so that the lead supervisory authority can be determined.

If the Company is based in an EU Member State or the UK and it makes decisions related to cross-border processing activities in the place of its central administration, there will be a single lead supervisory authority for the data processing activities carried out by the Company.

If Company has multiple establishments that act independently and make decisions about the purposes and means of the processing of Personal Data, top management of the Company needs to acknowledge that more than one lead supervisory authority exists.

### Main Establishment for the Data Processor

When the Company is acting as a data processor, then the main establishment will be the place of central administration. In case the place of central administration is not located in the Union, the main establishment will be the establishment in the Union where the main processing activities take place.

### Main Establishment for Non-EU Companies for DPOs and Processors

If the Company does not have a main establishment in the Union, and it has subsidiary(s) in the Union, then the competent supervisory authority is the local supervisory authority.

If the Company does not have a main establishment in the Union nor the subsidiaries in the Union, it must appoint a representative in the Union, and the competent supervisory authority will be the local supervisory authority where the representative is located.

# Response to Personal Data Breach Incidents

When the Company learns of a suspected or actual Personal Data breach, DPO must perform an internal investigation and take appropriate remedial measures in a timely manner, according to Netradyne Data Breach Response and Notification Procedure. Where there is any risk to the rights and freedoms of data subjects, the Company must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

# Audit and Accountability

The Privacy Oversight Team is responsible for auditing how well business departments implement this, Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

# Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which Netradyne operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

# Managing records kept on the basis of this document

| **Record name** | **Storage location** | **Person responsible for storage** | **Controls for record protection** | **Retention time** |
| --- | --- | --- | --- | --- |
| Data Subject Consent Attestation Forms | SharePoint/Privacy/ Data Subject Forms/ [Consent Attestations](https://netorg726775.sharepoint.com/:f:/s/Privacy/Esc-MCLY1OZPgAJ1HArAgZUB4I0nHt1o2aHSmrVGWD3fKg?e=QHOLRO) | DPO | Only authorized persons may access the forms | 10 years |
| Data Subject Consent Withdrawal Form | SharePoint/Privacy/ Data Subject Forms/ [Consent Withdrawals](https://netorg726775.sharepoint.com/:f:/s/Privacy/Eh2G44C9WctIhECE4oiAZbkB3FxBQ-PjhySCtcNh7tT16g?e=N6PeYN) | DPO | Only authorized persons may access the forms | 10 years |
| Supplier Data Processing Agreements | SharePoint/Privacy/ [Third Party](https://netorg726775.sharepoint.com/sites/Privacy/Third%20Party/Forms/AllItems.aspx) | General Counsel | Only authorized persons may access the folder | 5 years after the agreement has expired |
| Register of Privacy Notices | SharePoint/Privacy/ Data Subject Forms/ [Notices](https://netorg726775.sharepoint.com/:f:/s/Privacy/EvecpKEhrflBhAAgbFzpLm0BeMalOYY1LD1AubnRQBp41Q?e=7LfL5u) | DPO | Only authorized persons may access the folder | Permanently |

# Validity and document management

This document is valid as of February 03, 2025.

This document is approved by the DPO, who must check and, if necessary, update the document at least once a year.