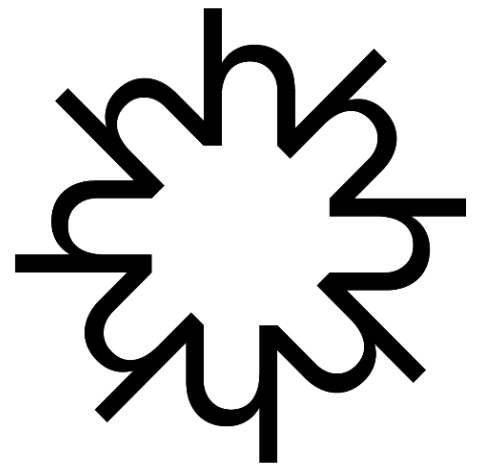


Data Protection Policy



horizont 3000



Content

1. Introduction	3
1.1 Purpose and Scope	3
1.2 Definitions	3
2. Principles of Data Protection.....	4
2.1 Requirements for Processing Personal Data	4
2.2 Data Protection by Design	5
2.3 Data Protection by Default.....	5
2.4 Data Transfer	5
2.5 Data Security	5
3. Data Collection and Processing.....	6
3.1 Data Subject Rights	6
3.2 Consent Management	6
3.3 Record Keeping of Consent.....	7
4. Data Breach Management	7
5. Training and Awareness	7
6. Monitoring and Compliance	8
7. Policy Review.....	8
8. Roles and Responsibilities of DPOs	8
8.1 h3 Data Protection Officer	9
8.2 Regional DPO Austria (DPO-AUT).....	9
8.3 Regional DPO Central America (DPO-AC)	10
8.4 Regional DPO East Africa (DPO-EA).....	10
8.5 Responsibilities of employees and contractors	11
8.6 Leadership Accountability.....	11
9. Contact Information.....	12
Annex 1: h3 data protection agreement for employees.....	13
Annex 2: h3 data protection agreement for contractors (Data Processing Agreement DPA)	13
Annex 3: Consent to Data Processing (Example Form).....	13
Annex 4: Consent to Data Processing in horizont3000's IT system	13
Annex 5: Specific tasks of the Regional DPO Austria (DPO-AUT)	13
Annex 6: Specific tasks of the Regional DPO Central America (DPO-AC).....	13
Annex 7: Specific tasks of the Regional DPO East Africa (DPO-EA)	14

1. Introduction

horizont3000 is committed to respecting and protecting personal data in alignment with its mission of sustainable development cooperation in its countries of activity. This Data Protection Policy (the "Policy") is intended to support compliance with data protection regulations in its country of activity, specifically in Austria, El Salvador, Guatemala, Kenya, Nicaragua, Tanzania, Uganda and the European Union. This Policy applies to all horizont3000 activities, employees, contractors, and partner organisations.

1.1 Purpose and Scope

This Policy outlines the principles and processes horizont3000 will follow to protect personal data. It covers data collection, processing, storage, security, and transfer practices to ensure individuals' privacy rights. The Policy applies to all data subjects, including employees, project participants, partners, and stakeholders working for horizont3000 and together with horizont3000.

1.2 Definitions

- **Personal Data:** Any information that relates to an identified or identifiable individual, as defined under the GDPR, Uganda Data Protection Act, Kenya Data Protection Act, Tanzania's laws, Personal Data Protection Act and Special Cybercrime Law of Nicaragua, Personal Data Protection Act and Cybersecurity & Information Security Act of El Salvador and/or other applicable laws.
- **Data Processing:** Any operation or set of operations performed on personal data, including collection, storage, transfer, and deletion. Data processing is not limited to electronic means, it includes written and spoken word.
- **Data Controller:** The person or role, who/which determines the purposes and means of processing personal data.
- **Data Processor:** An employee, a third-party organisation or a partner that processes personal data on behalf of horizont3000.
- **Data Subject:** A data subject is defined as an identifiable natural person, in the European Union General Data Protection Regulation (GDPR). A person can be identified directly and indirectly. A person can be directly identified through, for example, name or email address and indirectly through an online identifier (e.g. a given number).
- **Data Protection Officer (DPO):** The person or role responsible for overseeing data protection strategy and implementation in order to safeguard personal data and ensure the organisation adheres to the relevant requirements.

2. Principles of Data Protection

horizont3000 is committed to the following principles:

- **Lawfulness, Fairness, and Transparency:** Personal data will be processed lawfully, fairly, and transparently.
- **Purpose Limitation:** Data will only be collected for specific, legitimate purposes, clearly stated at the time of collection.
- **Data Minimization:** Only the minimum amount of data necessary will be collected and processed.
- **Accuracy:** Personal data will be kept accurate and up-to-date.
- **Storage Limitation:** Personal data will be stored only as long as the defined timeframe required to fulfill the purpose for which it was collected.
- **Integrity and Confidentiality:** Appropriate security measures will be implemented to prevent unauthorized access, processing, or destruction.
- **Security:** The implementation of appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data, protecting it against unauthorized access, alteration, disclosure, or destruction.
- **Transparency:** The obligation to provide clear, accessible, and comprehensive information to individuals about how their personal data is collected, used, stored, and shared, ensuring fairness and accountability in processing activities.
- **Participation:** The rights granted to individuals to actively engage in the processing of their personal data, including accessing their data, rectifying inaccuracies, erasing data, restricting processing, objecting to processing, and obtaining data portability, as well as being informed about and consenting to data use.
- **Accountability:** horizont3000 will maintain responsibility for data protection and compliance across all operations.

2.1 Requirements for Processing Personal Data

In compliance with applicable laws, horizont3000 will process personal data based on the following:

- **Consent:** Where required, explicit consent will be obtained before collecting and processing personal data.
- **Contractual Necessity:** Data processing necessary for the performance of a contract with data subjects.
- **Legal Obligation:** Processing required to comply with the relevant legal obligations.
- **Legitimate Interests:** Processing necessary for the legitimate interests of horizont3000, provided it does not override the rights of data subjects.

2.2 Data Protection by Design

When planning and developing our systems we shall incorporate data protection measures guided by the following principles:

- **Proactivity:** We Anticipate and prevent data protection risks instead of responding to incidents.
- **Privacy Safeguarding:** Integrating data protection features and principles into the design of systems and services.
- **Stringency:** Maintenance of data protection at every stage, from collection to deletion.
- **Risk Minimization:** Usage of measures like pseudonymization, encryption, and secure access to reduce exposure to risks.

2.3 Data Protection by Default

By default, only the minimum necessary personal data will be processed. It will be protected unless actively changed by the user or organisation. Key aspects:

- **Data Minimization:** We commit to collect and process only the personal data necessary for the specific purpose.
- **Default Privacy Settings:** We shall ensure systems and services are set to the most privacy-friendly settings by default.
- **Access Control:** We shall restrict access to personal data to only those who need it to perform their duties.
- **Purpose Limitation:** We commit to limit data processing to what is directly required for the stated purpose. This includes providing time-frames for automatic deletion of data.

2.4 Data Transfer

horizont3000 will ensure that all cross-border transfers of personal data comply with applicable data protection laws. Transfers will be conducted only with adequate safeguards, such as data protection agreements or standard contractual clauses as mandated by the GDPR.

2.5 Data Security

On the technical side, horizont3000 will use encryption, access controls, and secure storage systems to protect personal data. Organisationally, access to personal data is limited to authorized staff and partners. Security practices are subject to regular review and adaptation. We also ensure that partner organisations and data processors implement similar data protection measures through contractual agreements and the provision of safe mechanisms for data exchange.

Physical storage of data is governed by the corresponding data classifications schemes.

3. Data Collection and Processing

horizont3000 will:

- never process data collected for purposes that have not been agreed beforehand. Specifically, we will collect personal data directly from individuals whenever possible and inform them of the purpose.
- Limit data collection to essential information required for the specific purpose.
- Process data in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

3.1 Data Subject Rights

horizont3000 recognizes and will uphold the following rights of data subjects, as per the relevant data protection laws:

- **Right to Access:** Individuals can request access to their personal data.
- **Right to Rectification:** Individuals can request the correction of inaccurate data.
- **Right to Erasure:** Under Individuals can request the deletion of their data under conditions of GDPR and other applicable laws.
- **Right to Restrict Processing:** Individuals can request limitations on how their data is processed.
- **Right to Data Portability:** Individuals can request their data in a commonly used format.
- **Right to Object:** Individuals have the right to object to data processing under conditions of GDPR and other applicable laws.
- **Right to Withdraw Consent:** Individuals may withdraw consent at any time, where consent is the basis for processing.
- Requests by data subjects will be responded to promptly and within the legal timeframes as per applicable laws.

Requests by data subjects will be responded to promptly and within the legal timeframes as per applicable laws.

3.2 Consent Management

When obtaining consent, we ensure its validity by clearly specifying the purpose and ensuring the consent is specific, informed and unambiguous. Consent Forms are required to be in local language, plain and accessible, free from legal jargon. Our forms must provide:

- The identity of the data controller.
- The type of personal data being collected.

- The purpose of processing.
- The rights of the data subject.

Bundling consent for multiple purposes must be avoided.

Every data subject has the right to withdraw consent at any time. We ensure that the process is as easy as granting consent. A withdrawal of consent will result in an immediate cessation of any processing related to the withdrawn consent. Horizont3000 will confirm the withdrawal as well as the deletion or restriction of the relevant data, unless legally required to retain it.

horizont3000 will maintain detailed and accessible records that demonstrate when, how, and for what purpose consent was obtained from data subjects.

3.3 Record Keeping of Consent

The h3 Data Protection Officer (as defined in “Roles and Responsibilities”) is responsible for providing a secure and accessible process for Record Keeping of Consent. The Record Keeping itself is a shared responsibility between Regional Data Processing Officers (DPOs) and data processors (employees, partners, third party organisation).

- The data processor is required actively to collect and document consent in a form as required by the Regional DPO.
- The regional DPO is the data processor’s point of contact and responsible for administering record-keeping of consent in the specific region.

4. Data Breach Management

In the event of a data breach, horizont3000 shall undertake the following:

- Detection and Response: horizont3000 will promptly identify, contain, and mitigate any breaches;
- Notification: horizont3000 will notify the relevant authorities and affected data subjects as required by applicable laws, and;
- Record-Keeping: All data breaches will be documented, including the nature of the breach, corrective actions, and notifications made.

5. Training and Awareness

horizont3000 will provide regular data protection training for staff to promote awareness of data privacy obligations and encourage compliance with this Policy. Training will cover data protection principles, legal obligations, and security measures to protect personal data. They are to be held once per year at minimum.

6. Monitoring and Compliance

horizont3000 commits to monitoring compliance with this Policy and applicable data protection laws. The h3 Data Protection Officer, together with the Regional Data Protection Officers, will oversee adherence to data protection requirements, conduct regular audits, and ensure that any data processing agreements with third parties meet necessary legal standards.

7. Policy Review

This Policy will be reviewed annually, or more frequently, if necessary, to ensure it remains aligned with regulatory changes or operational needs. Updates to the Policy will be communicated to all staff and relevant stakeholders.

8. Roles and Responsibilities of DPOs

A **Data Protection Officer (DPO)** is an individual appointed to oversee an organisation's compliance with data protection laws and to ensure the protection of personal data during collection, processing, and storage.

Additionally the DPO is the first point of contact for employees, former employees, partners and donors.

h3 Data Protection Officer (DPO)

- GDPR compliance for globally available services
- Definition of Standards and a general Data Classification Scheme
- Interregional Reconciliation

Regional DPO Austria (DPO-AUT)

- Legal Compliance for data processing in Austria and the European Union
- Coordination with Austrian Workers Council
- Data Protection Trainings for h3 staff in Austria

Regional DPO Central America (DPO-AC)

- Legal Compliance for data processing in El Salvador, Guatemala and Nicaragua
- Data Protection Trainings for h3 staff in El Salvador, Guatemala and Nicaragua

Regional DPO East Africa (DPO-EA)

- Legal Compliance for data processing in Kenya, Tanzania and Uganda
- Data Protection Trainings for h3 staff in Kenya, Tanzania and Uganda

8.1 h3 Data Protection Officer

The h3 Data Protection Officer (DPO) is responsible for organisational policy and GDPR compliance of internal services, which are hosted for a global audience. The DPO is supported and advised by the Regional DPOs.

General tasks include:

- ↗ Maintain the data processors directory for services hosted worldwide
- ↗ Provide the process and secure storage for record keeping of consent
- ↗ Conduct data protection impact assessments for services hosted worldwide
- ↗ Define device standards regarding data protection and privacy
- ↗ Provide organisation-wide classification schemes for data
- ↗ Reconcile interests between organisational requirements and regional necessities
- ↗ Coordinate and adapt data protection measures with regional data protection officers
- ↗ Coordinate data protection measures with h3 internal labour representation bodies
- ↗ Keep basic understanding of the legal situation and peculiarities in all partner countries
- ↗ Keep track of data protection trainings

The DPO reports directly to the CEO.

8.2 Regional DPO Austria (DPO-AUT)

The Regional Data Protection Officer AUT (DPO-AUT) is in charge of GDPR compliance of systems and data hosted in Austria.

General tasks include:

- ↗ Monitor the legal situation in Austria and the European Union
- ↗ Maintain the data processors directory for services hosted and maintained in Austria
- ↗ Administer record keeping of consent for Austria and the European Union
- ↗ Conduct data protection impact assessments for services hosted and maintained in Austria
- ↗ Monitor compliance with device standards in regard to data protection and privacy
- ↗ Classify locally processed data in compliance with classification scheme

- Provide regional classification scheme adaptations (if required by applicable law)
- Coordinate data protection measures with Austrian Workers Council
- Conduct a data protection training for locally employed h3 staff at least once a year. This training can be provided by an IT specialist, hired by the RCO.

The DPO-AUT reports to the DPO.

8.3 Regional DPO Central America (DPO-AC)

The Regional Data Protection Officer Central America (DPO-AC) is in charge legal compliance of systems and data hosted in Nicaragua, Guatemala and El Salvador.

General tasks include:

- Monitor the legal situation in Nicaragua, Guatemala and El Salvador.
- Maintain the data processors directory for services hosted and maintained in Nicaragua, Guatemala and El Salvador.
- Maintain the data processors directory for services hosted and maintained in Nicaragua, Guatemala and El Salvador
- Administer record keeping of consent for Nicaragua, Guatemala and El Salvador
- Monitor compliance with device standards in regard to data protection and privacy
- Classify locally processed data in compliance with classification scheme
- Provide regional classification scheme adaptations (if required by applicable law)
- Conduct data protection impact assessments for services hosted and maintained in Nicaragua, Guatemala and El Salvador.
- Conduct a data protection training for locally employed h3 staff at least once a year. This training can be provided by an IT specialist, hired by the RCO.

The DPO-AC reports to the DPO.

8.4 Regional DPO East Africa (DPO-EA)

The Regional Data Protection Officer Central America (DPO-EA) is in charge legal compliance of systems and data hosted in Kenya, Tanzania and Uganda.

General tasks include:

- Monitor the legal situation in Kenya, Tanzania and Uganda.

- Maintain the data processors directory for services hosted and maintained in Kenya, Tanzania and Uganda.
- administer record keeping of consent for Kenya, Tanzania and Uganda
- Classify locally processed data in compliance with classification scheme
- Provide regional classification scheme adaptations (if required by applicable law)
- Conduct data protection impact assessments for services hosted and maintained in Kenya, Tanzania and Uganda.
- Conduct a data protection training for locally employed h3 staff at least once a year. This training can be provided by an IT specialist, hired by the RCO.

The DPO-EA reports to the DPO.

8.5 Responsibilities of employees and contractors

- Employees are required to sign the h3 data protection agreement for employees (Annex 1)
- Contractors are required to sign the h3 data protection agreement for contractors (Annex 2)

8.6 Leadership Accountability

horizont3000 requires its management to ensure compliance with data protection laws and principles throughout all levels of the organisation.

Persons in charge are expected to implement appropriate technical and organisational measures to guarantee and demonstrate that personal data processing activities adhere to GDPR requirements. This includes establishing comprehensive data protection policies, fostering a culture of privacy, providing necessary resources and training to employees, appointing a Data Protection Officer (DPO) when mandated, conducting Data Protection Impact Assessments (DPIAs) for high-risk processing, and ensuring that data subjects' rights are respected.

Leadership must also maintain documentation to demonstrate compliance and cooperate with supervisory authorities, embodying the GDPR's emphasis on accountability and transparency.

9. Contact Information

The Data Protection Officer can be contacted

<i>Region/Entity</i>	<i>Data Protection Officer</i>	<i>Contact</i>
<i>Organisation-Wide</i>	Stephan Walker	stephan.walker@horizont3000.org
<i>East Africa</i>	Solomon Mbubi	solomon.mbubi@horizont3000.org
<i>Central America</i>	Liliana Aragón	liliana.aragon@horizont3000.org
<i>Austria</i>	Stephan Walker	stephan.walker@horizont3000.org

Additionally, it is possible to use horizont3000's complaint mechanism at <https://www.horizont3000.org>. Your input will then be forwarded to the applicable Data Protection Officer.

Annex 1: h3 data protection agreement for employees

See attached document: 'h3 Data Protection Policy Annex 1'

Annex 2: h3 data protection agreement for contractors (Data Processing Agreement DPA)

See attached document: 'h3 Data Protection Policy Annex 2'

Annex 3: Consent to Data Processing (Example Form)

See attached document: 'h3 Data Protection Policy Annex 3'

Annex 4: Consent to Data Processing in horizont3000's IT system

See attached document: 'h3 Data Protection Policy Annex 4'

Annex 5: Specific tasks of the Regional DPO Austria (DPO-AUT)

There are no additional tasks to the general ones listed in Section 8.2.

Annex 6: Specific tasks of the Regional DPO Central America (DPO-AC)

Additionally to the general tasks listed in Section 8.3, the Regional DPO Central America has to make sure regional processes are in accordance with the following laws:

Country	Law number	Name of the Law	Date of approval and publication
Nicaragua	787	Personal Data Protection Act	<ul style="list-style-type: none"> Approved on March 21, 2012 Published in La Gaceta, Official Gazette No. 61 of March 29, 2012.
Nicaragua	1042	Special Cybercrime Law	<ul style="list-style-type: none"> Approved on October 27, 2020

			<ul style="list-style-type: none"> Published in La Gaceta, Official Gazette No. 201 of October 30, 2020
Nicaragua	1219	Law of Reforms and Additions to Law 1042, Special Cybercrimes Law	<ul style="list-style-type: none"> Approved on September 11, 2024 Published in La Gaceta, Official Gazette No. 170 of September 12, 2024
El Salvador	-	Personal Data Protection Act	<ul style="list-style-type: none"> Approved on November 12, 2024
El Salvador	-	Cybersecurity and Information Security Act	<ul style="list-style-type: none"> Approved on November 12, 2024
Guatemala	Decree 57-2008	Law on Free Access to Public Information*	<ul style="list-style-type: none"> Issued on September 23, 2008 Entered into force on April 20, 2009
		<p>* Although there is no specific legislation on personal data protection in Guatemala, the Law on Free Access to Public Information is currently the only one that regulates personal and sensitive data, as well as establishing a mechanism for their protection and criminalizing offenses in this area.</p>	

Annex 7: Specific tasks of the Regional DPO East Africa (DPO-EA)

Additionally to the tasks required in Section 8.4, the Regional DPO East Africa has the following responsibilities:

Ensure compliance with the Uganda Data Protection and Privacy Act, 2019, and the GDPR

- The DPO-EA must oversee all activities related to the collection, storage, processing, and sharing of personal data to ensure they align with the principles of lawful, fair, and transparent processing as outlined in **Section 3 of the Uganda Data Protection Act, 2019** and **Article 5 of the GDPR**. This includes ensuring that personal data is collected for specific, explicit, and legitimate purposes, stored securely, and not retained longer than necessary.

Facilitate the exercise of data subjects' rights

- Under **Section 24 of the Uganda Data Protection Act, 2019**, and **Articles 12–23 of the GDPR**, the DPO must enable data subjects to exercise their rights, including the right to access, rectify, delete, restrict processing, or object to the processing of their personal data. The DPO must establish procedures to handle requests promptly, ensure accurate documentation of responses, and communicate decisions effectively within the legal timelines.

Conduct and document Data Protection Impact Assessments (DPIAs)

- DPIAs are required under **Section 31 of the Uganda Data Protection Act, 2019**, and **Article 35 of the GDPR** for high-risk data processing activities. The DPO is responsible for evaluating the potential risks to personal data and recommending appropriate technical and organisational measures to mitigate these risks. This includes assessing new projects, technologies, or processes to ensure they are compliant by design and by default.

Act as the primary contact for the National Information Technology Authority - Uganda (NITA-U)

- As required under **Section 8 of the Uganda Data Protection Act, 2019**, the DPO serves as the official liaison with NITA-U. This role includes responding to inquiries, facilitating compliance audits, and submitting mandatory reports, such as data breach notifications. The DPO must also ensure that any requests or directives from NITA-U are implemented promptly and accurately.

Respond promptly to personal data breaches

- In compliance with **Section 28 of the Uganda Data Protection Act, 2019**, and **Articles 33–34 of the GDPR**, the DPO must develop and implement a robust data breach response plan. This includes identifying and containing breaches, notifying NITA-U within the prescribed timeframe (72 hours under GDPR), and communicating necessary details to affected individuals while advising them on mitigating potential risks.

Ensure timely renewal of the Personal Data Protection Officer (PDPO) certificate annually

- The Uganda Data Protection Act, 2019, requires organisations to have a certified PDPO. The DPO must track the expiration date of the certificate, prepare and submit all required documentation to NITA-U, and pay the necessary fees to ensure continued compliance. This role emphasizes maintaining the validity of certifications to uphold organisational legitimacy in data protection matters.

Collaborate with the Data Protection Officer at the headquarters

- In line with the **principle of accountability under Article 5(2) of the GDPR** and the broader organisational mandate under the Uganda Data Protection Act, 2019, the DPO must coordinate with the headquarters Personal Data protection Officer to harmonize policies, share updates on local legal developments, and address cross-regional compliance challenges. This collaboration ensures that Horizont3000 maintains consistent data protection standards across its offices while respecting local legal nuances.

Ensure compliance with the Uganda Data Protection and Privacy Act, 2019, and the GDPR:

- The DPO-EA must oversee all activities related to the collection, storage, processing, and sharing of personal data to ensure they align with the principles of lawful, fair, and transparent processing as outlined in Section 3 of the Uganda Data Protection Act, 2019 and Article 5 of the GDPR. This includes ensuring that personal data is collected for specific, explicit, and legitimate purposes, stored securely, and not retained longer than necessary.

Facilitate the exercise of data subjects' rights:

- Under Section 24 of the Uganda Data Protection Act, 2019, and Articles 12–23 of the GDPR, the DPO must enable data subjects to exercise their rights, including the right to access, rectify, delete, restrict processing, or object to the processing of their

personal data. The DPO must establish procedures to handle requests promptly, ensure accurate documentation of responses, and communicate decisions effectively within the legal timelines.

Conduct and document Data Protection Impact Assessments (DPIAs):

- DPIAs are required under Section 31 of the Uganda Data Protection Act, 2019, and Article 35 of the GDPR for high-risk data processing activities. The DPO is responsible for evaluating the potential risks to personal data and recommending appropriate technical and organisational measures to mitigate these risks. This includes assessing new projects, technologies, or processes to ensure they are compliant by design and by default.

Act as the primary contact for the National Information Technology Authority - Uganda (NITA-U):

- As required under Section 8 of the Uganda Data Protection Act, 2019, the DPO serves as the official liaison with NITA-U. This role includes responding to inquiries, facilitating compliance audits, and submitting mandatory reports, such as data breach notifications. The DPO must also ensure that any requests or directives from NITA-U are implemented promptly and accurately.

Respond promptly to personal data breaches:

- In compliance with Section 28 of the Uganda Data Protection Act, 2019, and Articles 33–34 of the GDPR, the DPO must develop and implement a robust data breach response plan. This includes identifying and containing breaches, notifying NITA-U within the prescribed timeframe (72 hours under GDPR), and communicating necessary details to affected individuals while advising them on mitigating potential risks.

Ensure timely renewal of the Personal Data Protection Officer (PDPO) certificate annually:

- The Uganda Data Protection Act, 2019, requires organisations to have a certified PDPO. The DPO must track the expiration date of the certificate, prepare and submit all required documentation to NITA-U, and pay the necessary fees to ensure continued compliance. This role emphasizes maintaining the validity of certifications to uphold organisational legitimacy in data protection matters.

Collaborate with the Data Protection Officer at the headquarters:

- In line with the principle of accountability under Article 5(2) of the GDPR and the broader organisational mandate under the Uganda Data Protection Act, 2019, the DPO must coordinate with the headquarters Personal Data protection Officer to harmonize policies, share updates on local legal developments, and address cross-regional compliance challenges. This collaboration ensures that Horizont3000 maintains consistent data protection standards across its offices while respecting local legal nuances.

Version 1.0: 2025

Next review: 2026

Approved by: horizont3000 Board

horizont3000, Austrian Organisation for Development
Cooperation, Wilhelminenstraße 9/II f, 1160 Wien, Austria