Data Processing Agreement (DPA)

Last updated on September 12, 2024

This Data Processing Agreement ("**DPA**") forms part of the Ory Network Terms and Conditions and the Ory Network Master Terms and Conditions for Enterprise Customers for all purposes to reflect the Parties' agreement related to Ory's processing of the Customer Personal Data. Capitalized terms used in this DPA not otherwise defined herein shall have the meanings set out in the Agreement.

1. **Safeguarding the Customer Personal Data**. Ory shall use commercially reasonable efforts to safeguard the security of the Customer Personal Data (which includes the Personal Data of the Customer's users), and shall employ for this purpose information security controls consistent with accepted practice in the industry, applicable law, and Appendix 1 (Technical and Organizational Measures to Ensure the Security of the Customer Personal Data).
2. **Privacy; Ory's Role as Service Provider**. Ory shall act solely as a service provider to the Customer under the Agreement, and Ory shall use the Customer Personal Data in accordance with the Agreement.
3. **Consumer Requests**. If Ory receives consumer requests related to the Customer Personal Data (including requests to delete or request to know, or similar, under applicable law), Ory's sole obligation will be to forward such requests to the Customer and the Customer shall be responsible for responding to and handling such consumer requests.
4. **Standard Contractual Clauses**. If Ory processes Personal Data of natural persons entitled to protection under the General Data Protection Regulation, then the standard contractual clauses set out in Appendix 2 (Standard Contractual Clauses) shall apply.

Appendix 1 to the DPA: Technical and Organizational Measures Designed to Ensure the Security of the Customer Personal Data

Ory uses the following technical and organisational measures to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

Topic	Practices
Organization of Information Security	**Security Ownership** Ory has appointed an individual to the role of a security officer for coordinating and monitoring Ory's security policies and procedures. **Security Roles and Responsibilities** Ory personnel with access to the Customer Personal Data are subject to confidentiality obligations. **Risk Management Program** Ory has established a formal Risk Management Program and maintains a Risk Register. Ory performs regular risk assessments and quarterly risk reviews with management. **Vendor Management** Ory has a vendor risk assessment process that is designed to implement vendor contract clauses and additional data protection agreements with vendors. **Security Assessments** Ory conducts internal and external security assessments on a regular basis and such security assessments are designed to ensure the effectiveness of security and compliance controls. These assessments may include audits, penetration testing and independent reviews of security professionals.
Asset Management	**Asset Inventory**

Topic	Practices
	Ory maintains an inventory of all asset on which the Customer Personal Data is stored. Access to such data is restricted to Ory personnel authorized to have such access. **Asset Handling** ● Ory classifies the Customer Personal Data to help identify it and to allow for access to it to be appropriately restricted. ● Ory communicates and enforces employee responsibility and accountability for data protection up to and including cause for termination. ● Ory personnel must obtain Ory's authorization prior to processing the Customer Personal Data outside of Ory's environments.
Human Resource Security	**Security Training** Ory requires all new hires to complete security and privacy awareness training as part of initial on-boarding. Participation in annual training is required for all employees to provide a baseline for security and privacy basics.
Physical and Environmental Security	**Physical Access to Facilities** Ory is not operating any data centers in its own facilities. Ory uses commercially reasonable efforts to ensures that physical access to the data centers of the cloud providers is secured in accordance with industry standards through a multi-layered approach and is regularly checked through Ory's Vendor Risk Assessment. **Protection from Disruptions** Ory uses commercially reasonable efforts to ensure that Ory's cloud providers use a variety of industry standards and best practices designed to protect against outages or failures of their own data centers. Ory Network uses redundancy throughout its setup, which is designed to eliminate single points of failure to ensure high availability.
Communications and Operations Management	**Operational Policy** Ory maintains security documents designed to describe its security measures and the relevant procedures and responsibilities of its personnel who have access to the Customer Personal Data. **Security & Privacy by Design** ● Ory follows a Security Development Lifecycle (SDL) program consisting of a set of practices that are designed to support security assurance and compliance requirements. The SDL helps developers build more secure software by reducing the number and severity of vulnerabilities in software, while reducing development cost. ● Ory follows the Privacy by Design principles with regular Privacy Impact Assessments. **Change Management & Configuration Management** ● Ory Network's configuration is managed in a version control system. Any change to its configuration is captured in an audit log. Changes to the production and staging environments require a strict approval process involving two or more employees. ● Changes applied to an Ory Network environment can be rolled back by reverting the change set in question. ● Promoting changes to the production environment requires the approval of the Change Advisory Board. **Anti-Malware Management / Malicious Software / Protective Technology** ● Ory validates that commercially reasonable Anti-Virus & Anti-Malware software is running on Ory-owned notebooks and devices.

Topic	Practices
	• The Ory Network locks down network communication to suppress non-standard communication in the cluster (Network Policies) • The Ory Network uses WAF solutions to actively prevent remote exploitation of vulnerabilities **Vulnerability & Patch Management** • Ory scans its own components during build time for known vulnerabilities and reports on any present vulnerability. • Ory scans all components (including used third party components) running in the Ory Network environments at runtime at least once a day and reports any vulnerabilities • Ory reviews the vulnerability management of the third party on a regular basis. • Ory utilizes a highly automated patch management tool that implements CI/CD pipelines and uses embedded approval workflows to apply changes to different environments. **Data Security in transit and at-rest** • The Ory Network encrypts data transferred to/from Ory Network using TLS 1.2 or higher • The Ory Network encrypts the Customer Personal Data at-rest using industry standard AES-256 encryption.
Access Control	**Access Policy** Ory maintains a record of security privileges of individuals having access to the Customer Personal Data. **Access Authorization** • Ory maintains and updates a record of personnel authorized to access Ory's systems that contain the Customer Personal Data. • Ory identifies those personnel who may grant, alter or cancel authorized access to the Customer Personal Data. • Ory has designed processes designed to ensure that where more than one individual has access to systems containing the Customer Personal Data, the individuals have separate identifiers/log-ins where technically and architecturally feasible, and commercially reasonable. **Least Privilege** • Technical support personnel are only permitted to have access to the Customer Personal Data when needed to perform their job functions. • Ory restricts access to the Customer Personal Data to only those individuals who require such access to perform their job function. Ory employees are only granted access to production systems based on their role within the organization. **Integrity and Confidentiality** • Ory instructs Ory personnel to disable administrative sessions when computers are left unattended. • Ory stores passwords such that they are encrypted or unintelligible while they are in force. **Authentication** • Ory uses industry standard practices to identify and authenticate users who attempt to access information systems.

Topic	Practices
	• Access to third party systems is secured using multi-factor authentication • Ory ensures that de-activated or expired employee identifiers are not granted to other individuals. • Ory monitors, or may (in Ory's sole discretion) enable the Customer to monitor, repeated attempts to gain access to the information system using an invalid password. • Ory maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. • Ory uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design** Ory has implemented controls designed to ensure no systems storing the Customer Personal Data are part of the same logical network used for Ory business operations.
Information Security Incident Management	**Incident Response Process** • Ory maintains a record of security incidents with a description of the incidents, the time period, the consequences of the breach, the name of the reporter, and to whom the incident was reported, and details regarding the handling of the incident. • In the event that Ory Security confirms or reasonably suspects that an Ory customer is affected by a data breach, Ory notifies the customer within a commercially reasonable period in accordance with applicable law • Ory tracks, or may (in Ory's sole discretion) enable the Customer to track, disclosures of the Customer Personal Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring** Ory employs a wide range of continuous monitoring solutions designed for preventing, detecting, and mitigating attacks to the site.
Business Continuity Management	• On an ongoing basis, but in no case less frequently than once a day, Ory maintains a backup of the Customer Personal Data from which the Customer Personal Data can be recovered. • Ory has implemented procedures governing access to copies of the Customer Personal Data. • Ory maintains emergency and contingency plans for the facilities in which Ory information systems that process the Customer Personal Data are located. • Ory's redundant storage and its procedures for recovering data are designed to attempt to reconstruct the Customer Personal Data in its original or last-replicated state from before the time it was lost or destroyed. • Ory performs testing of the disaster recovery capabilities on a regular basis.

Topic	Practices

Appendix 2 to the DPA: Standard Contractual Clauses

Annex I specifies the "data exporter" and "data importer"

SECTION I

Clause 1 - Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Annex to these Clauses referred to therein forms an integral part of these Clauses.

Clause 2 - Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Annex. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 - Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any

time, either as a data exporter or as a data importer, by completing the Annex and signing Annex I.A.

(b) Once it has completed the Annex and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Annex as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Appendix 1 to the DPA and personal data, the data exporter may redact part of the text of the Annex to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Appendix 1 to the DPA. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information

then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Appendix 1 to the DPA the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause - 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 - Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 - Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article

23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits.

It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18 - Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

LIST OF PARTIES

Category	Data Exporter	Data Importer
Party	Customer	Ory Corp
Business Address:	Provided on the Order Form	Provided on the Order Form

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- The Customer's prospects, customers, business partners and vendors (who are natural persons);
- The Customer's employees, contractors, agents, trade partners or contact persons of the Customer's prospects, customers, business partners and vendors (who are natural persons); and
- The Customer's employees, contractors, agents and advisors (who are natural persons).

Categories of personal data transferred

- Name (first and last);
- Job title;
- E-mail address;
- Telephone number; and
- Address.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The data is transferred on a regular and continuous basis.

Nature of the processing

Data is transferred electronically.

Purpose(s) of the data transfer and further processing

The data importer provides an identity management platform and related services. The data exporter intends to commission the data importer to provide certain Products and Material agreed to in the Agreement, including Ory will process data for the following purposes:

1. Storage and other processing necessary to provide, maintain and improve the Products and Material provided to the Customer; and/or

2. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data will be deleted in accordance with provisions of the Agreement, national law requirements, taking into account data storage obligations under applicable labor, tax and other regulatory laws.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Ory uses sub-processors to support its cloud environment and business operations. The Customer Personal Data processed by sub-processors is processed for the purposes and duration of the relevant services agreement between Ory and that sub-processor. Ory currently uses the following sub-processors:

Name and Address of the Sub-Processor*	Purpose of the Processing/Service Provided*	Countries where the Customer Personal Data will be Processed*
CloudFlare, Inc. 101 Townsend St, San Francisco, CA 94107 USA	DDOS Protection, Firewall, DNS, TLS, Rate-Limiting, CDN and Edge Worker Services	**Countries:** USA, United Kingdom, Singapore, Australia, Germany, Portugal, France, Japan, Canada, Netherlands, Dubai. **Subprocessors:** https://www.cloudflare.com/en-gb/gdpr/subprocessors/
Cockroach Labs, Inc. 125 W. 25th Street, 11th Floor New York, NY 10001 USA	Database Services	**Countries:** USA, Belgium, Germany **Subprocessors:**

Name and Address of the Sub-Processor*	Purpose of the Processing/Service Provided*	Countries where the Customer Personal Data will be Processed*
		https://www.cockroachlabs.com/cloud-terms-and-conditions/data-processing-addendum/cockroach-labs-sub-processors/
GitHub, Inc 88 Colin P Kelly Junior Street San Francisco, CA 94107 USA	Customer support	**Countries:** USA **Subprocessors:** https://docs.github.com/en/github/site-policy/github-subprocessors-and-cookies
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Cloud Service Provider: Storage, Compute, Managed Kubernetes, Network and Firewall functionality.	**Countries:** USA, European Economic Area **Subprocessors:** https://cloud.google.com/terms/subprocessors
HubSpot, Inc. 25 First Street, 2nd Floor Cambridge, MA 02141 USA	CRM Solution	**Countries:** USA **Subprocessors:** https://legal.hubspot.com/dpa
Mailgun Technologies 112 E. Pecan Street #1135, San Antonio, Texas, 78205 USA	Transactional mail services provider	**Countries:** USA, France, Sweden **Subprocessors:** https://www.mailgun.com/dpa/
Slack Technologies, LLC 500 Howard Street San Francisco, CA 94105 USA	Customer support communications	**Countries:** USA **Subprocessors:** https://slack.com/terms-of-service/slack-subprocessors
Stripe, Inc. 354 Oyster Point Boulevard South San Francisco, CA, 94080 USA	Credit card payment processing. Customers submit information directly to Stripe through Stripe's API. Ory does not handle credit card information.	**Countries:** USA **Subprocessors:** https://stripe.com/en-gb-de/service-providers/legal#list-of-affiliates
PostHog Inc 2261 Market Street #4008 San Francisco CA 94114 USA	Product Analytics using pseudonymist data	**Countries:** Germany **Subprocessors:** https://docs.google.com/document/d/1xfpP1SCFoI1qSKM6rEt9VqRLRUEXiKj9_0Tvv2mP928/edit
Functional Software, Inc., t/a 'Sentry' 45 Fremont Street, 8th Floor San Francisco CA 94105 USD	Application monitoring and error tracking	**Countries:** USA **Subprocessors:** https://sentry.io/legal/dpa/#list-of-subprocessors-1

Name and Address of the Sub-Processor*	Purpose of the Processing/Service Provided*	Countries where the Customer Personal Data will be Processed*
Zendesk, Inc. 989 Market St San Francisco, CA 94103	Customer support ticketing and communications	**Countries:** USA **Subprocessors:** https://support.zendesk.com/hc/en-us/articles/4408883061530-Sub-processor-Policy

COMPETENT SUPERVISORY AUTHORITY

New York, USA

DETAILS OF THE PROCESSING

1. **Nature and Purpose of Processing**. Ory will process the Customer Personal Data as necessary to perform its obligations in the Agreement and as otherwise contemplated in the Agreement.
2. **Duration of Processing.** Ory will process the Customer Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.
3. **Categories of Data Subjects**. The Customer Personal Data relates to the following categories of data subjects:
   - The Customer's prospects, customers, business partners and vendors (who are natural persons);
   - The Customer's employees, contractors, agents, trade partners or contact persons of the Customer's prospects, customers, business partners and vendors (who are natural persons); and
   - The Customer's employees, contractors, agents and advisors (who are natural persons).
4. **Type of Personal Data**.
   - Name (first and last);
   - Job title;
   - E-mail address;
   - Telephone number; and
   - Address.