

**DATA PROCESSING AGREEMENT**

To provide services, materials, or other resources (“Services”), HERE may Process Personal Data generated or collected by you on your behalf. This Data Processing Agreement (“DPA”) applies to Personal Data provided by you to HERE for Processing when HERE is acting as a Processor or subprocessor of Personal Data under a written agreement between you and HERE. This DPA assumes that you and/or your customers are Controllers with respect to any Personal Data that you provide to HERE for processing. HERE is only a Processor of that data for the sole purpose of providing Services to you.

**1. DEFINITIONS**

- 1.1 “Controller” means the natural or legal person (e.g., entity), public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- 1.2 “Breach” means any data privacy or security incident that meets the legal definition of a breach in Data Protection Law.
- 1.3 “Data Protection Law” means applicable regulations and legislation related to the protection of a Data Subject’s right to privacy and/or the fundamental rights and freedoms of Data Subjects.
- 1.4 “Data Subject” is a natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
- 1.5 “Personal Data” means any information relating to a Data Subject.
- 1.6 “Process,” “Processed,” or “Processing” means any operation or set of operations performed on or using Personal Data.
- 1.7 “Processor” means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of a Controller.

**2. DETAILS OF THE DATA PROCESSING**

You as the Controller determine the type and categories of Personal Data that HERE Processes on your behalf throughout your engagement of HERE Services. You as the Controller control the duration of the Processing; the nature and purpose of processing; and the type and categories of Data Subjects (e.g., your employees, contractors, suppliers, and/or end-users).

**3. RIGHT TO ISSUE INSTRUCTIONS**

HERE shall collect, process, and use Personal Data only in accordance with your documented instructions as set out in your written agreement with HERE. If your Processing instructions conflict with or infringe upon applicable law as determined by HERE, HERE will inform you of the conflict or infringement as soon as HERE becomes aware of it. HERE will only process Personal Data in accordance with Data Protection Law.

**4. PRIVACY MANAGEMENT**

HERE represents and warrants that it operates a comprehensive privacy program that includes (i) standards and processes intended to demonstrate HERE’s compliance with Data Protection Laws, regulations and contractual obligations; and (ii) effective processes for reviewing HERE standards and practices to ensure compliance. HERE ensures that its personnel and subprocessors engaged in the Processing of Personal Data are informed and have received appropriate training regarding their responsibilities and obligations of confidentiality, which survive the termination of its personnel or a subprocessor’s engagement with HERE. HERE shall ensure that access to your Personal Data is limited to those personnel who require such access to perform the Agreement. HERE’s global privacy and data protection team and Data Protection Officer may be reached via email at [privacy@here.com](mailto:privacy@here.com).

**5. TECHNICAL AND ORGANIZATIONAL MEASURES**

HERE implemented and maintains appropriate technical and organizational measures to ensure a reasonable level of protection based on ongoing risk assessments relate to the Processing Personal Data. These measures are documented in Exhibit A and regularly reviewed to include additional safeguards when needed. HERE is ISO 27001 certified and will maintain certification throughout the term of your written Service agreement with HERE. Evidence of HERE’s ISO 27001 certification is available to you upon request. HERE may implement different or additional technical and organizational measures and update the relevant description or documentation at any time without notice as long as the different or additional measures are not less protective than those already implemented either separately or in combination with other measures as determined by HERE’s ongoing risk assessments.

**6. YOUR OBLIGATIONS**

You shall comply with applicable Data Protection Laws including without limitation, (i) obtaining and maintaining all necessary registrations and authorizations with the competent data protection authorities; (ii) obtaining and maintaining all necessary and valid Data Subject consents or establishing other lawful grounds for the collection, Processing and sharing of Personal Data, where legally required; and (iii) observing all other data protection requirements. Without limiting the generality of the foregoing, you have sole responsibility for the accuracy, quality, integrity, legality, and reliability of the Personal Data and the means by which you acquired the Personal Data. HERE offers and makes available various security features and functionalities for you to use. If you choose to use these security features, you are responsible for properly configuring and using the Services (including security controls such as encryption) to ensure compliance with Data Protection Laws. This includes choosing security controls that are appropriate for the sensitivity of the Personal Data submitted.

## 7. ENGAGEMENT OF SUBPROCESSORS

You authorize HERE to subcontract the Processing of your Personal Data to subprocessors, as required for the functioning of HERE products and provisioning of the HERE Services. HERE's use of subprocessors is at HERE's sole discretion. Upon your request, HERE will inform you of the name, address, and role of each subprocessor used to process your Personal Data. HERE shall notify you in advance of any changes to the list of subprocessors in place on the effective date of the Services (except for emergency replacements or deletions of subprocessors without replacement). If you do not object within thirty (30) days after receipt of the list of subprocessors or within thirty (30) days of subsequent posted list updates, your consent to any changes to or additions of subprocessors will be deemed given. Upon receipt of your objection, HERE in its discretion may elect to cure the objection by: (1) not using the subprocessor; (2) taking the corrective steps you request to continue using the subprocessor; or (3) ceasing to provide the part or aspect of the Service conducted by the subprocessor or transferring the Personal Data out of the region that uses the subprocessor. If the objection has not been cured within thirty (30) days after HERE's receipt of your objection, either party may terminate Services upon thirty days' written notice. In case of subprocessing (including by affiliates of HERE), HERE shall: (i) enter into a written contract with its approved subprocessor that imposes at least equivalent obligations on the subprocessor as are imposed on HERE under this DPA and include a description of the technical and organizational measures that the subprocessor has to implement to ensure compliance with applicable laws and regulations; and (ii) ensure an adequate level of data protection within the meaning of the Data Protection Law by the subprocessor unless an adequate level of data protection is already ensured by Data Protection Law. Where legally required, HERE has entered into 'Standard Contractual Clauses' ("SCCs") for the transfer of personal data to processors established in third countries pursuant to Commission Decision 2010/87/EU prior to the subprocessor's Processing of Personal Data. The SCCs will be updated if and when the Commission updates the SCCs. HERE may also use subprocessors' modified SCCs that have been approved by a competent data protection authority. You hereby accede to HERE's use of SCCs with subprocessors on your behalf. HERE understands that it is liable to you if subprocessors do not meet their obligations under Data Protection Law and takes appropriate steps to ensure that subprocessors understand their obligations when Processing your Personal Data.

## 8. DUTIES TO NOTIFY

HERE shall inform you in writing without undue delay, but no later than 48 hours, after having become aware of any Breach. The written notification shall, to the extent available, include the following: (i) the date of the Breach; (ii) a description of the Breach; and (iii) any additional information required by law. If any such information is not available at the time of its initial notification, HERE shall supplement its notification as its investigation progresses. In case of a Breach, HERE shall refrain from making any regulatory filings or publishing any notifications relating to the Breach without your written authorization unless required by applicable law and shall at its own expense thoroughly investigate the Breach and take appropriate measures to mitigate or remedy the situation.

## 9. DUTIES TO ASSIST

HERE shall notify you without undue delay regarding any received Data Subject requests, that can reasonably be identified as pertaining to you. HERE shall provide reasonable assistance to you within technical and legal constraints in responding to Data Subject requests if HERE Services do not permit you to respond to the requests on your own. If HERE receives a request from a law enforcement or other governmental agency for disclosure of Personal Data, HERE will direct that request to you and promptly notify you of such requests or complaints unless prohibited by law. Unless required by law, HERE shall not respond to an agency request or complaint involving your Personal Data without your written approval of the response.

## 10. AUDIT RIGHTS

You may audit HERE's security practices regarding the Processing of your Personal Data only, if: (i) HERE has not provided a copy of its ISO 27001 certification or other contracted standard(s); (ii) a Breach has occurred; (iii) you have reasonable grounds to believe that HERE is not complying with its obligations under this DPA; (iv) an audit is formally requested by your competent data protection authority; or (v) Data Protection Law provides you with a direct audit right. You shall provide HERE with at least sixty (60) days of advance notice. If the advance notice of at least sixty (60) days is provided, HERE shall provide reasonable support for the audit. Reasonable support means that your audit shall be limited to one business day without disrupting HERE's regular course of business and shall be subject to HERE's reasonable security and confidentiality requirements. Each Party shall bear its own audit costs.

## 11. EXPIRATION OR TERMINATION OF AGREEMENT

After termination or expiration of the Service agreement(s), HERE shall, at your sole discretion and within thirty (30) days after the termination or expiration, delete or destroy the Personal Data, including any copies, in accordance with Data Protection Law and your instructions. HERE shall confirm its compliance with the foregoing. All Processing of your Personal Data will cease and no further processing shall be permitted.

**Exhibit A – HERE Technical and Organizational Measures**

To ensure that personal rights and freedoms are safeguarded in the Processing of Personal Data, HERE has implemented the following technical and organizational measures:

**SECURITY POLICIES AND MANAGEMENT**

- HERE senior management assigns security responsibilities and reviews the implementation of security within the organization. Senior management has nominated an individual responsible for the overall security, risk management, information security, privacy, and controls for Processing of Personal Data.
- HERE demonstrates its commitment to data security through its development and implementation of an organization-wide security policy (“Security Policy”). This Security Policy and related guidelines are communicated to all employees working on your engagement of HERE.
- HERE has implemented an internal information classification schema based on data or information sensitivity and has established practices to ensure that information ownership is defined and appropriately limited. This schema includes appropriate security controls to protect your information based on ongoing risk assessments that allow HERE to modify controls and measures as needed.
- HERE conducts security risk assessments at least annually that review and take into account emerging threats, potential business impacts, and probabilities of occurrence. HERE modifies the security related processes, procedures, and guidelines based on the findings in such security risk assessments.

**INDEPENDENT CERTIFICATIONS AND AUDIT RIGHTS**

For production systems that run the Services provided to you, HERE maintains its ISO 27001 certification. Upon your request or at least annually, HERE provides an update about applicable certifications and reports, including any identified deficiencies for your review. Such information and copies thereof are Confidential Information as defined in the HERE Platform Terms.

**SECURITY INCIDENT MANAGEMENT**

HERE has developed and implemented effective issue and incident response procedures and has clearly identified individuals and their responsibilities to ensure that HERE is able to react quickly to resolve potential vulnerabilities and incidents, and minimize potential damage by security or privacy threat actors. HERE notifies and escalates events related to unauthorized disclosure, modification, or misuse of your Personal Data. HERE shall use agreed incident communications channels in communicating the incident(s) in a timely fashion. HERE shall attempt to mitigate the incident, related to your Personal Data, already at the time of noticing and shall report to you only such incidents which cannot be excluded from being identified as false alerts. HERE shall have competent people to conduct investigations.

**EMERGENCY RESPONSE AND BUSINESS CONTINUITY**

HERE has a documented and implemented up-to-date emergency response plans for all Services. These plans ensure the availability and integrity of Services as well as the safety of people, premises, and assets. HERE’s Emergency Response and Business Continuity Plans are communicated throughout HERE as applicable and necessary. HERE also develops contingency plans and has appropriate workaround solutions in place for ensuring compliance with Service Level Agreements (SLAs). HERE’s Emergency Response and Business Continuity Plans are tested as part of HERE’s Business Continuity testing cycle.

**PERSONNEL AND SUBCONTRACTOR SECURITY**

- HERE’s personnel, subcontractors, and other external service providers shall have valid, signed, written confidentiality agreements in place to ensure their understanding of their obligations prior to accessing HERE’S environments and systems where your Personal Data is processed. HERE shall ensure that there is a verifiable and auditable trail of confidentiality agreements at all times between you, HERE and their subcontractors and/or external service providers.
- HERE ensures that there is an appropriate entry and exit procedure for personnel changes that includes granting and disabling of user access and returning of assets when terminating the employment with HERE or upon personnel changes related to Services provisioning targeted to you.

**AWARENESS**

HERE conducts security and privacy awareness trainings (or refresher sessions) during induction and thereafter at least annually to all relevant existing employees and new hires. HERE ensures that due emphasis is given to the handling of client confidentiality and specifically unlaunched product information and social media guidelines (and restrictions).

**IT SECURITY**

- HERE has implemented appropriate access control and access rights management designed to ensure that data is only processed by a minimum number of authorized persons who have access to requisite data needed to perform their work-related duties (i.e., role-based access control with least privileges).
- HERE maintains the following: processes for authorizing and terminating user access and subcontractor access, including emergency access termination procedure; password management policy including password complexity requirements, no common or shared user accounts in use, password aging where systems do not support use of password managers, and secure delivery of credentials to users; audit records of all existing user privileges, shall be retained and reviewed regularly to remove excess privileges, and processes which ensure segregation of duties.
- HERE further maintains a sufficient audit trail and the use of access privileges (changes, who, what, when) is in place when dealing with sensitive (confidential or secret) information.
- HERE collects logs pertaining to user access to your Data and stores such logs for at least three (3) months unless otherwise restricted by local legislation.
- HERE has implemented reasonable and appropriate information security measures (e.g., hardening, patching, antivirus, IDS, etc.) to protect your Data against unauthorized or accidental access, use, disclosure, deletion, destruction, loss, alteration, or amendment.
- HERE only stores and processes your Data in an environment where requisite security controls have been implemented. HERE ensures that IT infrastructure and networks are designed and managed to protect IT systems, information, users, and electronic communications.
- HERE uses industry standard techniques to secure the connectivity between you and HERE against eavesdropping and alteration (including wireless access or remote connection), in solutions and services provided by HERE.