Data Privacy Policy

Experts in perimeter protection

Privacy Policy

This privacy policy (the “privacy policy”) provides details of the way in which Heras B.V. (“the company”,) processes personal data when you work for the company or when you do business with the company.

Personal data is processed in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) and other applicable national and European privacy legislation and regulations (together the “data protection law”).

Terms in bold used in this privacy policy are defined in the glossary in Annex I.

1. Scope

This privacy policy applies to all personal data we process as a data controller.
To the extent the company decides why and how personal data is processed, the company is a data controller of such personal data.
The company may process personal data of, for example, employees, former employees, and their family members, temporary workers, self-employed persons, job applicants, contractors, supplier contacts, customers, and visitors.

2. Purspose

The purpose of this privacy policy is to explain what personal data we process and how and why we process it. In addition, this privacy policy outlines our duties and responsibilities regarding its protection.
This privacy policy is not an exhaustive statement of our data protection practices, we will give you notice of variations to the extent practical.
[to the extent that national data protection law (the “national law”) is relevant to this privacy policy, and/or [insert company name] (the “company”) processes personal data in any manner that is different to what is set out in this privacy policy (e.g. Regarding the categories of personal data processed, purposes of processing, etc.,) details of such specific processing are set out in Annex II.]

1. Type of personal data

1.1 Employees and Contractors

The company collects and processes personal data in relation to our employees, candidates for employment and contractors, as well as our former employees and former contractors. This personal data includes: personal details such as name, date of birth, social security number, bank account details, next of kin, details of social media accounts, visa / passport data; contact details such as address and phone number(s); personnel file details including, for example, terms and conditions of employment, training, performance evaluations, promotions, personal development plans, conduct and disciplinary data, work location, salary information, bank account details and tax and social security numbers, security clearances; employment history/application details such as educational history and employment history; editorial or journalistic content such as links to works e.g. links to video files or audio files; medical information such as medical certificates and sick notes; family details such as names and dates of birth of children (e.g. Relevant if an individual is applying for parental leave); details required for pension; details regarding trade union membership; and performance related data such as performance management ratings for managers and annual incremental salary reviews of employees, psychometric testing, etc.
The above list is not exhaustive but covers the most commonly collected, used and otherwise processed personal data.

1.2 Suppliers and Customers

The company collects and processes personal data in relation to individuals who are, and/or are working with, our suppliers and customers. This personal data may include: personal details such as name, title, position, work identification numbers, department, business unit (including contact data collected for training / verification); and contact details such as email address, telephone number(s) and work location; and tax information such as vat / tax numbers.

1.3 Special Categories of Personal Data

The types of special categories of personal data that the company may process includes, without limitation, health data, information on criminal convictions and biometric data. The company processes all personal data in accordance with data protection law, and, in particular, any special categories of personal data.
[further details of the types of personal data and special categories of personal data processed us are set out in Annex II.]

2. Purposes of processing

The company processes personal data for the purpose(s) for which the personal data has been obtained.

Common examples of the reasons why the company processes personal data include: payroll and benefit administration; HR, performance and talent management; marketing and PR; improvement of business products and services; research and statistical analysis; business strategy; internal audits or investigations; prevention and detection of unlawful and/or criminal behavior towards us or our customers and employees; and/or fulfilling legal obligations. We may process personal data for other reasons from time to time. The company tries to ensure individuals are informed about the purpose(s) for processing their personal data at the time the company collects consent. Where this is not possible or practical, the company tries to inform you as soon as possible after the processing of personal data. Individuals have the right to withdraw consent at any time.

3. Profiling

The company may process the personal data of various individuals (for example, employees, contractors and candidates for employment) for talent management and workforce evaluation (to potentially include attendance and performance analysis).
The company engages in such processing where: (a) expressly authorised by national law (including for fraud and tax-evasion monitoring); (b) necessary for the entering into or performance of a contract; or (c) the individual has given appropriate consent. [further details of the type of profiling we do are detailed in Annex II.]

4. Individual rights

Individuals have certain rights under data protection law.

4.1 Inspection and Access: you can request from us a summary and a copy of your personal data which we process or which is processed on our behalf;
4.2 Correction/Addition/Removal: where you believe your personal data is inaccurate or incomplete, you are entitled to request us to correct, amend or delete your personal data;
4.3 Objection: you may object to us processing your personal data based on our legitimate reasons for processing (see section 2 PURPOSES OF PROCESSING above);
4.4 Restriction: you may request that we restrict the processing of your personal data where the accuracy of your personal data is contested, our processing is unlawful, you believe we no longer need the personal data or you have objected to processing; and
4.5 Automated Decision Making: where the company undertakes automated decision making (including profiling), which significantly affects you, you are entitled to object to such decision-making.

The company's Individual's Data Protection Rights and Requests explain how the above requests can be made and how the company will manage these requests.

5. SECURITY

5.1 Security Measures

The company has technical and organizational measures in place to protect personal data from unlawful or unauthorized destruction, loss, change, disclosure, acquisition or access. Personal data are held securely using a range of security measures including, as appropriate, physical measures such as locked filing cabinets and privacy by design in systems.

For more information on the company's security measures, please see the Global Information Security Policy as implemented on 1st of January 2018 and the yearly updates [and Annex II].

5.2 Personal Data Breach

The company will manage a data breach in accordance with the personal data breach reporting procedure. For guidance on how to identify and report a data breach please refer to our Personal Data Breach Procedure.

6. DISCLOSING PERSONAL DATA

From time to time, the company may disclose personal data to third parties, or allow third parties to access personal data which we process (for example where a law enforcement agency or regulatory authority submits a valid request for access to personal data).

The company may also share personal data: (a) with another member of the HERAS B.V. (including our subsidiaries, our ultimate holding company and its subsidiaries); (b) with selected third parties including business partners, suppliers and sub-contractors; (c) with third parties when we sell or buy any business or assets; or (d) if the company is under a legal obligation to disclose personal data. This includes exchanging information with other companies and organizations for the purposes of fraud prevention.

Where the company enters into agreements with third parties to processes personal data on our behalf it will ensure that the appropriate contractual protections are in place to safeguard it. Examples include communications providers, payroll service providers, occupational health providers, marketing or recruitment agencies, operators of data centers used by the company, etc. [Further details of the categories of third parties to which the company discloses individuals' personal data are set out in Annex II.]

7. Data retention

The company keep personal data only for as long as the retention of such personal data is deemed necessary for the purposes for which that personal data are processed. Personal data is retained in accordance with relevant laws and company guidelines. [further details of the retention period for personal data followed by the company (or the criteria used to determine such retention period) are set out in Annex II.]

8. Data transfers outside the EEA

From time to time the company may need to transfer the personal data outside the EEA. This transfer will occur in accordance with applicable data protection law. The company takes reasonable steps to ensure that the personal data is treated securely and in accordance with this privacy policy when transferred outside the EEA. [further details of the nature of the data transfers undertaken by the company are set out in Annex II.]

9. Roles and responsibilities

The company is responsible for the processing of personal data. The company's managing director has overall responsibility for the company's compliance with this privacy policy and will designate a primary point of contact in relation to (i) the processing of personal data of the company's current and former employees and contractors; (ii) the processing of personal data of business contacts; and (iii) the preservation of the security and integrity of the personal data processed by the company.

Legal and Compliance shall provide support to the company by providing legal advice and guidance in interpreting the data protection law and this privacy policy on a local level.

All company employees must comply with the most up-to-date version of this privacy policy, as published from time to time. If employees are found to have intentionally violated this privacy policy, they may be subject to disciplinary processes, up to and including dismissal.

10. Complaints procedure

You can ask a question or make a complaint about this privacy policy and/or the processing of your personal data by contacting the country HR manager at HERAS B.V.

Annex I

GLOSSARY

In this privacy policy, the terms below have the following meaning:

"CCM" means the country compliance manager for the company;

"Cross-border processing" arises where: (a) we are established in more than one EU member state and our processing of personal data takes place in more than one EU member state; or (b) while our processing of personal data takes place in only one EU member state, this processing substantially affects (or is likely to substantially affect) individuals in more than one EU member state.

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"Data controller" means the entity that decides why and how personal data is processed.

"Data processor" means the party that processes personal data on behalf of the data controller (for example, a payroll service provider).

"European Economic Area" or "EEA" means Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the UK, Iceland, Liechtenstein, and Norway.

"Personal data" is any information relating to a living individual which allows the identification of that individual. A person is identifiable if his/her identity can reasonably be established from the data without any disproportionate effort. Personal data can include:

Employees and Contractors

1. Personal details such as name, date of birth, bank account details, next of kin, details of social media accounts;
2. Contact details such as address and phone number(s);
3. Personnel file details including, e.g, terms and conditions of employment, training, performance evaluations, promotions, personal development plans, conduct and disciplinary data, work location, salary information, bank account details and tax and personally identifiable numbers such as a social security numbers;
4. Employment history/application details such as educational history and employment history;
5. Editorial or journalistic content such as links to works, e.g. Links to show-reels or audio files;
6. Medical information such as medical certificates and sick notes;
7. Family details such as names and dates of birth of children, e.g. Relevant if an individual is applying for parental leave;
8. Details required for pension;
9. Details regarding trade union membership; and
10. Performance related data such as performance management ratings for managers and annual incremental salary reviews of employees, psychometric testing, etc.

Suppliers and Customers

1. Personal details such as name, title, position, work identification numbers, department, business unit;
2. Contact details such as email address, telephone number(s),
3. Work location; and
4. Tax information such as vat / tax numbers.

"Processing" includes collecting, using, recording, organising, altering, disclosing, destroying or holding personal data in any way. Processing can be done either manually or by using automated systems such as information technology systems and "process" and "processing" shall be interpreted accordingly.

"Profiling" is the automated processing of personal data for the purpose of assessing certain aspects relating to an individual so as to analyse or predict the individual's performance, decisions or behaviour.

"Special Categories of Personal Data" are types of personal data that reveal any of the following information relating to an individual: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Special categories of personal data also include the processing of genetic data, biometric data (for example, fingerprints or facial images), health data, data concerning sex life or sexual orientation and any personal data relating to criminal convictions or offences.

Annex II

Company specific processing 1

This annex contains additional information in respect of the way in which the company processes personal data.

1. Relevant local law and data protection regulator

In this annex, "data protection law" means the General data protection regulation (regulation (eu) 2016/679) and the Dutch data protection Act. In respect of the company the relevant local data protection regulator is: The Dutch Data Protection Authority

2. Personal data processed by the company

In addition to those categories of personal data detailed in section 1 of the privacy policy, the company also processes the following categories of personal data: data with regard to the license plate of a lease car

3. Purposes of processing personal data

In addition to those purposes detailed in section 2 of the privacy policy, the company also processes personal data for the following additional purposes: no additional purposes

4. Profiling

The company engages in the following types of profiling: G

5. Security measures

The company implements the following additional technical and organizational security measures to protect the personal data from unauthorized destruction, loss, change, disclosure, acquisition or access: no additional security measures

6. Disclosure of personal data to third parties

The company discloses or provides access to the personal data to the following additional categories of third party for the purposes explained below: no additional categories

7. Data retention periods

The company retains personal data on the basis of the document Archive policy – Overview retention periods, kind and terms, HERAS B.V.

8. Data transfers

The company transfers personal data to the locations outside the EEA, for the purposes specified in the company's Personal Data Register, using the stated legal safeguards (a copy of which are available from the Group HR Director)

Individuals' data protection rights and requests

The General Data Protection Regulation ("GDPR") provides for a wide range of rights for individuals in respect of their personal data (the "Individual Rights"). As a result, individuals may make requests to review, edit, delete, correct or object to the processing of their personal data.

The purpose of this document is to: (1) explain what these Individual Rights are; and (2) explain how to manage a request from an individual to exercise such Individual Rights (a "request") in compliance with the GDPR or other applicable laws. The flowchart in the Appendix to this document will assist in illustrating how requests can be managed.

1. Individual rights

The Individual Rights under the GDPR include:

A. Right of Access

Each Heras Country/Division as a Data Controller, upon specific request by an individual, is required to:

- confirm if it processes the individual's personal data;
- explain why and how it is processing that individual's personal data and provide other details to the individual in respect of the processing of that individual's personal data; and
- provide a copy of the personal data to that individual.

B. Right to Erasure (also known as the right to Delete or "the right to be forgotten") and Rectification

An individual may request his/her personal data be 'erased' or deleted in certain circumstances including if, at any time, he/she withdraws his/her consent to the processing of his/her personal data (where the processing is conducted pursuant to the consent of the data subject). The individual can also require the Heras Division to "rectify" or amend his/her personal data if it is inaccurate or incomplete.

If the Heras Division has shared the personal data with any third party (for example, a data processor such as a payroll provider), then the Heras Division must notify such third party of the erasure or restriction of the relevant personal data.

C. Right to Restriction

An individual may also require the Heras Division to limit the processing of his/her personal data whilst complaints (for example, about accuracy of the personal data) are being dealt with. When processing is restricted, the Heras Division is permitted to store the personal data, but not further process it unless or until the matter is resolved. Similarly, if the Heras Division has shared the personal data with any third party (for example, a data processor such as a payroll provider), then the Heras Division must notify such third party of the restriction imposed on processing the personal data of the relevant individual until further notice. Upon lifting the restriction, the third party must also be notified.

D. Right to Object

Individuals may object to the processing of their personal data on grounds relating to his or her particular situation. The Heras Division then needs to stop processing this personal data, unless it can demonstrate compelling legitimate grounds for the processing (to be

determined on a case-by-case basis).

However, individuals can object without having to provide any justification if an Heras Division is processing for direct marketing purposes.

If a decision is made on automated processing of personal information, including profiling, and where that decision is likely to produce legal effect on the individual or which could significantly affect him/her, the individual has the right not to be subject (save for some specific exceptions) to a decision being made solely on that basis. Examples of such automated processing are online credit decisions.

E. Data Portability

If an individual provides the Heras Country / Division with his or her personal data, that individual has the right, upon request:

• to receive a copy of the personal data; and/or

• where technically feasible, to have the personal data sent to a third party organisation in a structured and commonly used automated format

2. Managing requests

A. Responding to a request

The Heras Division must communicate with the individual who has made the request, and with any third party to whom the personal information had been shared, once the amendment, deletion or restriction has been carried out.

Information or communications provided to individuals in response to a request need to be:

• in a concise, clear, easy to understand and easily accessible format, using plain language;

• in writing (e.g. by letter or email); and

• where an individual makes a request in electronic form (e.g. by email), the response may also be provided in electronic form (i.e. by email) where possible unless the individual requests otherwise.

B. Deadline for responding to a request

After receipt of a valid request, the response must be provided "without undue delay" but, in any event, not later than one month after receipt of the request. That one month period may be extended by a further two months where necessary, taking into account the complexity and number of requests. The Heras Division must inform the individual of any such extension within the first month of receipt of the request, together with the reasons for the delay/extension.

If the Heras Division has a valid and legitimate reason for not responding to a request either within the prescribed timeframe, or at all, it must: (a) inform the individual "without delay" of the reasons for not taking any action but, in any event, not later than one month after receipt of the request; and (b) inform the individual of his/her right to file a complaint with the relevant data protection authority.

C. Costs for responding to a request

All information/communications by the Heras Division in relation to a request must be free of charge unless the request from the individual is "manifestly unfounded or excessive" (for example, repeated requests), in which case the Heras Division may: (a) charge a reasonable fee to the individual; or (b) refuse the request.

D. Any questions?

If you have any questions or need further guidance, the Heras Country HR can raise queries with Group HR or Group IT about the interpretation of this procedure.

Personal data breach procedure

1. Introduction

This personal data breach procedure (the "procedure") describes the process for escalating, reporting and recording suspected or actual data breaches involving personal data (as defined below). This procedure applies to Heras (the "company"). The purpose of this procedure is to ensure that the company manages and contains any personal data breach (as defined below) quickly so that the impact of the data breach can be minimised and any legal obligation to report the data breach to a regulator and/or any individual(s) affected by the data breach (in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR")) can be complied within good time.

2. What is personal data?

Personal data is any information relating to a living individual (located within the European Economic Area) which is capable of identifying that individual ("personal data"). A person is identifiable if his/her identity can reasonably be established from the data without any disproportionate effort. Examples of personal data include: name, address, date of birth, telephone number, account number, job title, photo, IP address, etc.

3. What is a personal data breach?

The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" ("personal data breach"). A personal data breach occurs when there is any unauthorised or accidental disclosure, loss or any other form of unauthorised, accidental or unlawful collection, use, recording, storing or distributing of personal data. Examples of personal data breaches are: loss or theft of a laptop or mobile phone which contains personal data; sending an (unprotected) excel file with personal data to an unauthorised person; printing wage details and subsequently leaving them on a printer; hacking of a system containing personal data; and/or loss or theft of files; etc.

An incident involving a breach of data security is described as a "data incident". If a data incident does not involve personal data, it is not a personal data breach. Furthermore, not all data incidents involving personal data will be personal data breaches. For example the loss or compromise of personal data may not qualify as a personal data breach where: (i) the personal data is encrypted or anonymised; (ii) there is a full, up-to-date back-up of the personal data; and (iii) access to the personal data is monitored. Accordingly, the determination of whether a data incident constitutes a personal data breach must be made on a case-by-case basis.

4. When does this procedure apply?

If personal data is not involved in the data incident, this procedure will not apply. If personal data is involved in the data incident, a personal data breach may have occurred and this procedure will apply. If there is any doubt as to whether a personal data breach has occurred, the company should immediately seek advice from country HR Manager to assess the situation promptly.

5. How do i report a personal data breach internally?

It is important that all actual or suspected personal data breaches are immediately reported internally within Heras B.V. in accordance with the following steps:

5.1 Initial reporting

Upon becoming aware of an actual or suspected personal data breach, this should be immediately reported to the Financial and IT Director (the "Company Director") or Group HR. The company Director shall promptly report any actual or suspected personal data breach to Legal and Compliance.

5.2 Response planning

If a personal data breach has occurred, the company Director, or a delegate, shall work together with Legal and Compliance to develop a plan to respond to the personal data breach. Annex A sets out a flowchart for managing a personal data breach.

In developing the relevant response plan, the response team will consider:

- the information received in the personal data breach notification;
- the required actions to be immediately taken to contain the personal data breach;
- whether there is a requirement to notify the relevant data protection authority ("DPA (+31) - (0)70 - 888 85 00") of the personal data breach and if so, what needs to be reported;
- the potential consequences for the company and the impacted individuals arising from the personal data breach;

• the measures which the company is taking at that time and/or can take to mitigate damage to the impacted individuals;
• the manner by which the impacted individuals will be informed of the personal data breach, if appropriate in the circumstances, and the measures which the individuals can take to mitigate further damage;
• whether there might be personal liability, or liability of third parties, arising from the personal data breach;
• internal (and, if necessary, external) communications and the timing of such communications;
• whether, apart from the DPA, other stakeholders should also be informed; and
• what learning might be taken from the personal data breach and what measures can be implemented to seek to prevent any reoccurrence.

5.3 Notification to the DPA required?

Not every personal data breach needs to be reported to the DPA. For example, it is not necessary to notify the DPA where the personal data breach is unlikely to result in a risk to any individual(s).

If it is necessary to report the personal data breach to the relevant DPA, Legal and Compliance shall report the personal data breach to the relevant DPA after having discussed this with the company Director.

The report to the relevant DPA should be made without undue delay, and where feasible, not later than 72 hours after having become aware of the personal data breach. If notification is not made within 72 hours, a reasoned justification for the delay must be provided to the DPA.

5.4 Resolution

Following notification to the relevant DPA and considering any observations from that DPA, Legal and Compliance shall consult with the company Director in relation to the management and resolution of the personal data breach in accordance with the relevant personal data breach response plan.

6. What needs to be reported to the PDA?

In making a report, the DPA must be informed of:
• the nature of the personal data breach, including the categories of personal data and individuals involved, the number of impacted individuals and the amount of compromised personal data;
• the likely consequences to be expected from the personal data breach;
• the measures taken or proposed to be taken to address the personal data breach;
• the measures that can be taken by the impacted individuals to limit harmful consequences arising from the personal data breach; and
• the name and contact details of the Heras B.V. point of contact from whom more information regarding the personal data breach can be obtained.

7. Personal data breach notification to impacted individuals

The impacted individual will only need to be informed if a personal data breach is likely to result in a 'high risk' to the rights and freedoms of the data subject. Reporting of the personal data breach to the impacted individuals shall take place in accordance with the relevant response plan.

The notification sent to the impacted individuals will include, at the least: (i) the nature and extent of the data breach; (ii) the measures taken to limit the negative consequences of the personal data breach; (iii) a description of the consequences both established and assumed of the personal data breach for personal data; and (iv) the measures which the company has taken or proposes to take to mitigate the consequences of the personal data breach.

Notification to individuals will not be required where: (a) the company has implemented appropriate technical and organisational measures that render the personal data unintelligible to anyone not authorised to access it, such as through use of encryption; or (b) the company has taken subsequent measures which ensure that the high risk to individuals is not likely to materialise.

8. Data breach register

The company must maintain a register which records all personal data breaches. HR and IT will keep a register of personal data breaches notified to it by the company.

The purpose of the register of personal data breaches is: (i) to learn from the personal data breach and from the way in which it was dealt with; (ii) to be able to provide accurate answers to questions received from impacted individuals and/or the DPA as appropriate; and (iii) to provide a summary to the DPA if requested to do so.

For each personal data breach, the following will be captured on the register:

- date and time of reporting of the personal data breach;
- name and contact details of the impacted individual(s);
- the facts and details of the nature of the personal data breach;
- to whom the personal data breach has been reported and why; and
- the follow-up actions after discovery of the personal data breach (such as any measures to prevent the personal data breach reoccurring, etc.).

The company's register of any personal data breaches reported to the DPA must be retained for at least five years.

Published by	Heras
Contact Person	Country HR Manager
Purpose	Ensure transparent and compliant business conduct
Application / Distributed to	All employees
Classification	Public
Monitoring	Executive committee
Version	V_1.1
Signed off by / on	Board Heras