HES Privacy Policy

Index

1. Introduction

Scope

This Policy applies to HES International B.V., its direct or indirect, wholly- and majority-owned subsidiaries and all its employees, directors, officers (full or part time or temporary), consultants, agents and representatives ("**HES**").

This Policy and its implementation may be supplemented by local policies or guidelines designed to ensure that a local subsidiary meets additional requirements applicable to it under local data protection or other laws.

Purpose

The EU General Data Protection Regulation 2016/679 ("**GDPR**") is designed to harmonise data privacy laws across Europe in order to protect and empower all EU citizens' personal data. The GDPR applies to all the processing of personal data in the context of the activities of an establishment in the EU, regardless of whether the processing takes place in the EU or not.

Under the GDPR, any information related to an identified natural person or identifiable (directly or indirectly) natural person qualifies as personal data. Information does not have to be 'personal' or 'private' in nature to be considered personal data under the GDPR, meaning that information relating to individuals in their professional rather than their personal capacity can also be regulated by the GDPR. In addition, the fact that information is not processed along with the respective individual's name does not mean that such information is not considered personal data. As long as the individuals can be identified by other means, all information relating to them will be considered personal data.

Pursuant to the GDPR, the processing of personal data includes almost any action done with personal data, i.e. the collecting, sending, accessing, saving, copying, changing and any way of using personal data.

The purpose of this Privacy Policy is to ensure that HES' business activities are conducted in accordance with the GDPR. In addition to being a legal requirement, the lawful and proper care of any personal data is a fundamental component of the 'HES Code of Conduct' and our overarching corporate values.

2. Privacy statements

Individuals whose personal data is being obtained and processed ("**data subjects**") have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. To that extent, all individuals must be provided with a privacy statement at the time their personal data is collected from them. This obligation also applies *vis-á-vis* the employees of HES. If personal data is obtained from other sources, individuals must be provided with a privacy statement

within a reasonable period from obtaining the data and no later than one month. It is not necessary to provide data subjects with a privacy statement if they already have the information or – in the event the data is obtained from other sources – if it would involve a disproportionate effort to provide it to them. Privacy statements must contain the information contained in the privacy statements provided in **Appendix 1** and must also be available in the language of the country in which the privacy statements are provided.

3. Data protection impact assessments

What is a data protection impact assessment?

By law, in a number of circumstances HES (as a data controller, *verwerkingsverantwoordelijke*) is required to carry out a data protection impact assessment (a "**DPIA**") of the impact and potential risks its envisaged processing could have to data subjects, in particular when carrying out potentially high-risk, or bulk, processing of personal data. Controllers must: (i) describe the processing, (ii) where appropriate, explain the reasons for that processing, (iii) assess the necessity and proportionality of the processing, together with the risks to data subjects resulting from its processing of their personal data.

A DPIA should identify effectively, and then resolve, any areas of concern at an early stage, and always before processing commences.

The systematic and prescribed use of DPIA's throughout HES is an integral part of our compliance program as it demonstrates that HES has carefully and properly considered any potential or actual risks presented by the data processing.

What types of data processing require a DPIA?

A DPIA does not need to be conducted for every data processing activity. A risk-based approach is required and a case-by-case analysis as to when a DPIA is required or desirable should be undertaken.

The GDPR requires a DPIA where data processing "is likely to result in a high risk to the rights and freedoms of natural persons". Examples of when a DPIA will be required are:

- A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
- Processing on a large scale of sensitive personal data, including personal data relating to criminal convictions and offences.
- New technologies are being used on a large scale (geographical scale or number of data subjects).

Other examples of the types of projects that may require a DPIA include:

- A new IT system or other arrangement for processing, storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system.
- A new database which consolidates information held by separate parts of an organisation.

If you believe that a DPIA may be required, please review the HES Data Protection Impact Assessment Policy and consult with the legal department of HES International B.V. (the "**Legal Department**") if so required.

4. Security and data protection

The following technical and organisational measures must be in place in order to ensure that the data processing and the data protection is at a sufficiently secure level:

- Data back-ups
- Network security
- Network authentication
- Network segmentation
- Antivirus / Antimalware / Firewalling
- Regular software updates
- Limited access to personal data through role-based access control / password-controlled folders
- Security and reception personnel screening
- Timely deleting of personal information, please review the HES Document Retention Policy

The level of the technical and organisational measures applied must be proportionate to – among others - the severity of the risks to the data subjects involved in the data processing activities.

5. Design and assessment of processing arrangements

Where a new information technology system or other arrangement involving the processing of personal data ("**processing system**") is to be implemented, or a significant change is to be made to an existing processing system, the person with overall responsibility for that processing system should:

- ensure that full account is taken of the requirements of this Privacy Policy and the privacy of data subjects in the selection, design and implementation of the new elements of the new or changed processing system, including in particular:
    - seeking to keep the personal data to be processed by the processing system to the minimum level consistent with HES' business and other requirements; and
    - where personal data are to be processed and this is reasonably practicable and consistent with those requirements, keeping data allowing the identification of data subjects separate from other elements of the relevant personal data, and effectively protected, so that the data subjects are not identifiable except where this is necessary for HES' business or other purposes; and
- conduct an assessment of the implications of this Policy for HES' processing of personal data in that processing system, and its implications for the privacy of data subjects, to ensure that, following the implementation or change, the processing system will comply with the principles set out in this Privacy Policy in all respects and, generally, that its implementation will not result in high risks for the privacy of the relevant data subjects.

If an assessment concludes that a proposed new or changed processing system may give rise to high risks to the privacy of the relevant data subjects, please review the HES Data Protection Impact Assessment Policy and consult with the Legal Department is so required.

6. Personal data breach notification procedure

Scope

A data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Personal data breaches can include:

- access to personal data by an unauthorised third party;
- sending personal data to an unintended recipient;
- lost or stolen devices containing personal data;
- loss of availability of personal data.

All personal data breaches must be documented.

In case of a personal data breach, all employees, contractors or temporary employees are required to be aware of, and follow, the following procedure.

Procedure

1. The personal data breach must be contained and recovered.
2. Documentation of the breach should take place as it develops.
3. The potential severity of the impact on the data subject(s) involved must be assessed.
4. The Legal Department must be notified as soon as possible on the same day of the breach. This notification shall at least:
    a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
    b) describe the likely consequences of the personal data breach;
    c) describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
5. The Legal Department will investigate whether or not the breach has to be reported to the supervisory authority.
6. If required, the Legal Department will notify or will arrange for a notification to the supervisory authority in accordance with Article 33 and, if necessary, Article 34 of the GDPR.

7. Data subject rights and request procedure

Scope

Data subjects have the right:

- to be provided with a copy of any personal data that HES holds about them, with certain related information;
- to require HES, without undue delay, to update or correct any inaccurate personal data, or complete any incomplete personal data, concerning them;
- to require HES to stop processing their personal data for direct marketing purposes; and
- to object to the processing of their personal data more generally.

Data subjects may also have the right, in certain circumstances:

- to require HES, without undue delay, to delete their personal data;
- to "restrict" HES' processing of their personal data, so that it can only continue subject to very tight restrictions; and

- to require personal data which they have provided to HES, and which are processed based on their consent or the performance of a contract with them, to be "ported" to them or a replacement service provider.

A request does not have to include the phrase 'data subject access request', ‘Article 15 of the GDPR’, ‘data portability’ or ‘Article 20 of the GDPR’ as long as it is clear that the individual wishes to exercise their rights under the GDPR. The GDPR does not specify how to make a valid request. Therefore, an individual can make a request verbally or in writing. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point. Consequently, all employees, contractors or temporary employees are required to be aware of, and follow, the following procedure in case of a data subject request. All data subject requests must be documented and please also take into account the HES Internal Guidance on Data Subject Requests.

Procedure

1. Identify the individual making the request. If you have doubts about the identity of the person making the request, you must ask them for more information. However, it is important that you only request information that is necessary to confirm who they are. Proportionality is key.
2. Documentation of the request should take place as it develops.
3. Check whether the request is manifestly unfounded, excessive or repetitive, in which case a reasonable fee (based on the incurred administrative costs) may be charged for complying with the request. You must obtain the requestor’s confirmation for the fee to be charged before taking further action. Please note that it is HES who must prove that the request was manifestly unfounded, excessive or repetitive. Therefore, you must assess each request carefully, and must use this exception only in very limited cases.
4. You must contact the Legal Department if – from the context of the request – it may be determined that the data subject wishes to exercise the following rights:

    a. right to object to the processing of their personal data other than for direct marketing purposes;

    b. right to deletion (erasure) of personal data;

    c. right to restriction of the processing of personal data;

    You must comply with the Legal Department's instructions when responding to such requests.
5. You must act on the data subject request without undue delay and at the latest within one month of receipt. Where requests are complex or numerous, you are permitted to extend the deadline to the extent necessary to respond to the request, but only up to three months. However, you must still respond to the request within a month to explain why the extension is necessary. Please also note that it is HES who must prove that such extension was necessary.

6. You must ensure that a written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response.

8. Processing register

All personal data processing activities must be documented in an electronic processing register. In order to correctly reflect the processing activities, the processing register must be kept up to date and shall contain – among others - the following information:

1. The purpose of the processing.
2. A description of the categories of data subjects and of the categories of personal data.
3. The categories of recipients to whom the personal data have been or will be disclosed.
4. Where possible, the envisaged time limits for erasure of the different categories of data.
5. Where possible, a general description of the technical and organisational security measures.

Please review the HES Data Processing Register Template.

9. Agreements with processors

When a third party ("**processor**") is used to process personal data on your (as the "**controller**") behalf, a written data processing agreement to that extent must be in place. In this regard, a 'third party' may also be another HES company in specific circumstances. A data processor can be for example a hosting service provider managing the company's website, or an accountant.

The agreement with the processor is important so that both parties understand their responsibilities and must include the following terms:

- the processor must only act on the written instructions of the controller, including with regard to transfers of personal data outside the European Economic Area (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations under Article 28 of the GDPR, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Where HES engages a processor, it must:

- conduct appropriate due diligence on the technical and organisational security arrangements that the processor have in place to protect the personal data disclosed to that processor; and
- take reasonable steps (for example by exercising audit rights and/or making enquiries of the processor) to ensure that the security measures required of the processor are in place in practice over time during the life of the relevant processing arrangement.

Please review the HES Data Processing Agreement Template.

10. Standard GDPR clause for commercial contracts

Given the possibility of personal data processing covered by the GDPR in the execution of commercial storage and handling contracts, we advise to incorporate a standard GDPR clause in commercial contracts. Such a clause should, at least, contain the following: "*The parties may provide each other with information related to an identified or identifiable individual ("Personal Data"), the processing and transfer of which will be done in accordance with applicable data protection law. The Parties agree and acknowledge that they will act as separate data controllers in respect of any Personal Data processed under this Agreement.*"

11. International data transfers

HES will only transfer personal data outside the European Economic Area (EEA):

- where the transfer is to a country or other territory which has been assessed by the European Commission as ensuring an adequate level of protection for personal data;
- where the data subjects have given their explicit consent to the transfer taking place; or
- where the Legal Department has approved the transfer on the basis that it is compliant with the GDPR and other applicable laws.

For the purposes of this Policy, a transfer is any transfer of personal data. This includes arrangements through which a person outside the EEA has remote access to personal data stored within the EEA.

12. Code of conduct for ISPS and AEO requirements

Following to International Ship and Port Facility Security Code ("**ISPS**") requirements for terminals and requirements for companies certified as an Authorized Economic Operator ("**AEO**"), security measures are in place which involve the processing of personal data. The HES terminals must have a Code of Conduct in place which describes the GDPR compliant execution of security measures in light of ISPS and AEO certificates.

13. ADM policy

Information regarding the alcohol, drugs or medicine ("**ADM**") blood levels and information regarding (suspected) ADM use/abuse of an individual qualifies as sensitive personal data. Consequently, such personal data must be processed by or under the responsibility of a professional subject to the obligation of professional secrecy and this Privacy Policy must be accounted for in the ADM policies in place. The processing of such data must also comply with all applicable local laws.

14. Co-operation with Data Protection Authorities

Each HES company is obliged to co-operate with the competent data protection authorities in the EU in the performance of their tasks. Any communication received from a competent data protection authority should be passed to the Legal Department as soon as is reasonably practicable.

15. Contact

If you have any (possible) questions or concerns about this privacy policy you may contact the Legal Department by sending an e-mail to compliance@hesinternational.eu

***

ANNEX 1

HES Privacy Statement

Employees / Applicants / Contractors

Please ensure that the lists below is up-to-date and complete.

Insert HES entity and all its direct and indirect subsidiaries ("***") possesses and will collect personal data about you both prior to, during and after of your employment relationship, if you apply for a position at Insert HES entity and if you work for us on a contracting basis. Insert HES entity respects your privacy and will treat your data in compliance with the applicable employment laws and data protection laws, including the General Data Protection Regulation. In this policy we describe how and for what purposes Insert HES entity collects and uses your personal data.

The companies processing your personal information are:

Insert HES entity

1. WHOSE... personal data is being used?

HES entity collects and handles personal data in relation to amongst others employees, contractors, temporary workers, applicants, as well as related family members or other contact persons (for emergency purposes).

2. WHAT... personal data is being used?

Personal data, or personal information, means any information relating to an identified or identifiable natural person. Depending on the circumstances, we may collect, store, and use (all together: process) the following categories of your personal information:

- Personal contact details such as name, title, addresses, telephone numbers, and email addresses.
- Date of birth.
- Gender.

- Social security number / citizen service number / BSN number.
- Identification document number.
- Marital status and dependents.
- Next of kin and emergency contact information.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date(s) of job roles.
- Location of employment or workplace.
- Copy of identity documents, such as passport, driving license, utility bills.
- Recruitment information (including copies of right to work documentation, references and other. information included in a C.V. or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Salary/payments history.
- Performance information, also including assessment results and references..
- Disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Photographs.

We may also process more sensitive personal information (to the extent permitted by applicable laws) about your health relevant to your work, including, for example, any medical condition, working capacity and absence records (other than holidays).

This personal data will be updated from time to time, for example by receiving new information from you directly. It is important that the personal information we hold about you is accurate and up-to-date. Please keep us informed if your personal information changes during your working relationship with us.

3. WHY… is your personal data being used?

We will only process your personal information when the law allows us to and/or requires us to do so.

We are required by law to have a ground set out in the law to process the information we hold about you. When you are working at HES entity, or apply for a position here, our processing of your personal information is based on the following legal grounds:

(a) the performance of a contract to which the data subject is a party or in the performance of pre-contractual measures resulting from a request by you and which are necessary for entering into a contract, such as your employment agreement;

(b) the processing is necessary to comply with legal or regulatory obligations (such as required disability administration in the event of a long-term period of occupational disability);

(c) the processing is necessary to secure a vital interest of yours (such as emergency contact information for your next of kin in the event of an emergency); and/or

(d) the processing is necessary in the legitimate interests of HES entity in exercising its and its staff fundamental rights to run a business in a way which does not unduly affect your interests or fundamental rights and freedoms. When processing is necessary for the legitimate interests of HES entity, we ensure that processing is conducted in such a manner that our legitimate interests outweigh any individual's interest.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

The company collects and processes personal information:

(a) To fulfil our obligations to you as an employer or individual contractors when you commence work for HES entity and when you start working for HES entity, which means that we will comply with your employment agreement or services agreement, and all other arrangements that we have agreed around your employment agreement. This includes:

- Making a decision about your recruitment or appointment (including confirming if you are legally entitled to work);
- Career development and performance assessment (including education and making decisions about salary reviews and compensation);
- Workforce planning (which includes (i) ascertaining your fitness to work, e.g. drug and alcohol testing; (2) managing sickness absence, (3) complying with (internal and legal) health and safety obligations), (4) to use information relating to leaves of absence, which may include sickness absence or family related leaves, and (5) to use information about your physical or mental health, or disability status to ensure your health and safety in the workplace, to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- Transfer of employees;

- Management reporting;
- Succession planning;
- Disciplinary matters;
- Equal opportunities monitoring;
- Administration of salaries and benefits;
- Calculation and payment of tax;
- Legal and compliance purposes; and
- any other purposes as may be required in connection with the performance and execution of your employment agreement

(b) Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.

(c) Business management and planning, including accounting and auditing

(d) Promote the security and protection of people, premises, systems and assets. This includes:

- To monitor your use of our information and communication systems to ensure compliance with our IT policies;
- To ensure network and information security, including preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution;
- To conduct data analytics studies to review and better understand employee retention and attrition rates;

(e) Monitor compliance with internal policies and procedures. This includes our activities to prevent fraud;

(f) Administer communications and other systems used by HES entity (including internal contact databases);

(g) Investigate or respond to incidents and complaints;

(h) Comply with obligations and rights and cooperate with investigations carried out by the police, government or regulators; and

(i) To transfer data to third parties (see also below);

4. WHAT… happens if you do not provide any personal data?

When our request for your personal information is a legal or contractual obligation, or a requirement necessary to enter into a contract, and you fail to provide that personal information, the consequence could be that you are not allowed to enter offices, we cannot enter into a contract with you (or your employer or a company related to you) or we have to suspend the execution of our contract with you (or your employer or a company related to you).

5. WHOM... does HES entity share my personal data with?

We may share your personal information with third parties to complete the set of purposes that we have explained above. Third parties includes third-party service providers (including contractors and designated agents) and other entities within the HES International group. All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our privacy policy. We do not allow our third-party service providers to use your personal information for their own purposes. We only permit them to process your personal information for specified purposes and in accordance with our instructions.

The following activities could be carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services, and recruitment services. All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our privacy policy.

We may share your personal information with other entities within the HES International group as part of our regular reporting activities on company and/or group performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data, or where we consider that another group entity is better placed to consider your suitability for a potential role. We may also share your personal data with a person who takes over our business and assets or relevant parts of them.

In exceptional circumstances, we may also share your information the competent regulatory, prosecuting and other governmental agencies, or litigation counterparties, in any country or territory.

6. DOES... HES entity share my personal data outside the European Economic Area?

We do not transfer your personal information outside the European Economic Area.

7. WHAT... does HES entity do to protect my personal information?

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They may only process your personal information on our instructions and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

8. HOW... long does HES entity store my personal information?

HES entity aims to only collect the minimum amount of personal data required. We will only keep your personal information for as long as necessary to fulfil the purposes we collected it for. The specific period depends on the reason why we have your personal data. We determine this period in line with our HES Document Retention Policy.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker, contractor or candidate or an individual working at a clients or potential client of ours, we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

9. WHAT... rights do I have?

Under certain circumstances as defined by law, you have the right to:

- **Request access** to your personal information (also known as a "data subject access request"). You can ask us whether we process any of your personal data. If we do this, you can request to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request to be forgotten**. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing of your personal information** where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing of your personal information**. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer of your personal information** to you or a third party in a structured, commonly used and machine-readable format (also known as "right to data portability").

If you want to make use of any of these rights, you may contact the compliance officer, please refer to section 10. You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

10. WHO... can I contact if I have questions or concerns?

If you have any (possible) concerns on this privacy statement you may report these to the Chief Compliance Officer (compliance@hesinternational.eu). You can also contact your local compliance officer in case of any questions or requests.

You also have the right, at any time, to lodge a complaint about our processing of your personal information with a data protection authority. The relevant contact information can be found here: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

11. HOW... do you handle changes to this privacy notice?

This privacy statement will be reviewed and in addition may be reviewed from time to time to take account of, for example, changes to legislation, regulatory developments and organizational changes.

A new privacy statement will be provided to you when any substantial changes are made. We may also notify you in other ways from time to time about the processing of your personal information.

12. Update history

VERSION	REVISED BY	DESCRIPTION	REVISION DATE

ANNEX 2

HES Privacy Statement

Third Parties

Please ensure that the lists below is up-to-date and complete.

HES entity and all its direct and indirect subsidiaries ("***") possess and will collect personal data about you both prior to, during and after your affiliation with HES entity. HES entity respects your privacy and will treat your data in compliance with the applicable employment laws and data protection laws, including the General Data Protection Regulation. In this policy we describe how and for what purposes HES entity collects and uses your personal data.

The companies processing your personal information are:

HES entity

1. WHOSE... personal data is being used?

HES entity collects and handles personal data in relation to (potential) clients, visitors and website visitors.

2. WHAT... personal data is being used?

Personal data, or personal information, means any information relating to an identified or identifiable natural person. Depending on the circumstances, we may collect, store, and use (all together: process) information that you give us (for example by filling in forms on our website or corresponding with us by phone, e-mail or otherwise) or information that we collect from you (for example, when you visit our website the web server collects some basic information such as your browser type). The personal data that we process may include the following categories of your personal information:

- Personal contact details such as name, title, addresses, telephone numbers, and email addresses.
- Information about your business relationship with HES entity, and information about your professional role, background and interests. If we have a business relationship with the

organisation that you represent, your colleagues or other business contacts may give us information about you such as your contact details or details of your role in the relationship.

- If you visit our website it will automatically connect some information about you and your visit, including the anonymized Internet protocol (IP) address used to connect your device to the Internet and some other information such as your browser type and version and the pages on our site that you visit. Read further information on our website. https://www.hesinternational.eu/en/cookie-statement
- License plate number.
- We sometimes collect information from third party data providers or publicly available sources for anti-money-laundering, background checking and similar purposes, and to protect our business and comply with our legal and regulatory obligations.

This personal data will be updated from time to time, for example by receiving new information from you directly. It is important that the personal information we hold about you is accurate and up-to-date. Please keep us informed if your personal information changes during your working relationship with us.

Please ensure that the list above is up-to-date and complete.

3. WHY… is your personal data being used?

We will only process your personal information when the law allows us to and/or requires us to do so.

We are required by law to have a ground set out in the law to process the information we hold about you. Our processing of your personal information is based on the following legal grounds:

(a) when you have given us your consent to process your personal data;

(b) the performance of a contract to which the data subject is a party or in the performance of pre-contractual measures resulting from a request by you and which are necessary for entering into a contract;

(c) the processing is necessary to comply with legal or regulatory obligations;

(d) the processing is necessary to secure a vital interest of the data subject or of another natural person (such as emergency contact information for your next of kin in the event of an emergency); and/or

(e) the processing is necessary in the legitimate interests of HES entity in exercising its and its staff fundamental rights to run a business in a way which does not unduly affect your interests or fundamental rights and freedoms. When processing is necessary for the legitimate interests of HES entity, we ensure that processing is conducted in such a manner that our legitimate interests outweigh any individual's interest.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.
If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.
We will only process your personal information as necessary so that we can pursue the purposes described above, and then only where we have concluded that our processing does not prejudice you or your privacy in a way that would override our legitimate interest in pursuing those purposes.
In exceptional circumstances we may also be required by law to disclose or otherwise process your personal information.
We will tell you, when we ask you to provide information about yourself, if provision of the requested information is necessary for compliance with a legal obligation or, on the other hand, if it is purely voluntary and there will be no implications if you decline to provide the information. Otherwise you should assume that we need the information for our business or compliance purposes (as described below).
The company collects and processes personal information: Please confirm that the list below is complete.

(a) Determining or agreeing with you (or your employer or a company related to you) the terms on which we work together.

(b) Providing contractual benefits to you.

(c) Administering the contract we have entered into with you.

(d) Business management and planning, including accounting and auditing.

(e) Conducting performance reviews, managing performance and determining performance requirements.

(f) To contact you about your or our service requirements.

(g) Making arrangements for the termination of our contractual relationship.

(h) Dealing with legal disputes involving you.

(i) Complying with (internal and legal) health and safety obligations.

(j) To contact you with information about (y)our services.

(k) To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

(l) To operate, administer and improve our website and premises and other aspects of the way in which we conduct our operations.

(m) To protect our business from fraud, money-laundering, breach of confidence, theft of proprietary materials and other financial or business crimes; and

(n) To comply with our legal and regulatory obligations and bring and defend legal claims.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information. We may from time to time review information about you held in our systems – including the contents of and other information related to your email and other communications with us – for compliance and business-protection purposes as described above.

Your emails and other communications may also occasionally be accessed by persons other than the member of staff with whom they are exchanged for ordinary business management purposes (for example, where necessary when a staff member is out of the office or has left HES entity).

4. WHAT… happens if you do not provide any personal data?

When our request for your personal information is a legal or contractual obligation, or a requirement necessary to enter into a contract, and you fail to provide that personal information, the consequence could be that you are not allowed to enter our offices, we cannot enter into a contract with you (or your employer or a company related to you) or we have to suspend the execution of our contract with you (or your employer or a company related to you).

5. WHOM... does HES entity share my personal data with?

We may share your personal information with third parties to complete the set of purposes that we have explained above. Third parties includes third-party service providers (including contractors and designated agents) and other entities within the HES International group. All our third-party service providers are required to take appropriate security measures to protect your personal information in line with the HES Privacy Policy. We do not allow our third-party service providers to use your personal information for their own purposes. We only permit them to process your personal information for specified purposes and in accordance with our instructions.

We may share your personal information with other entities within the HES International group as part of our regular reporting activities on company and/or group performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data. We may also share your personal data with a person who takes over our business and assets or relevant parts of them.

In exceptional circumstances, we may also share your information the competent regulatory, prosecuting and other governmental agencies, or litigation counterparties, in any country or territory.

6. DOES... HES entity share my personal data outside the European Economic Area?

We do not transfer your personal information outside the European Economic Area.

7. WHAT... does HES entity do to protect my personal information?

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They may only process your personal information on our instructions and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

8. HOW... long does HES entity store my personal information?

HES entity aims to only collect the minimum amount of personal data required. We will only keep your personal information for as long as necessary to fulfil the purposes we collected it for. The specific period depends on the reason why we have your personal data. We determine this period in line with the HES Document Retention Policy.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker, contractor or candidate or an individual working at a clients or potential client of ours, we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

9. WHAT... rights do I have?

Under certain circumstances as defined by law, you have the right to:

- **Request access** to your personal information (also known as a "data subject access request"). You can ask us whether we process any of your personal data. If we do this, you can request to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request to be forgotten**. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing of your personal information** where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing of your personal information**. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer of your personal information** to you or a third party in a structured, commonly used and machine-readable format (also known as "right to data portability").

If you want to make use of any of these rights, you may contact the Chief Compliance Officer or the local compliance officer, please refer to section 10. You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

10. WHO... can I contact if I have questions or concerns?

If you have any (possible) concerns on this privacy statement you may report these to the Chief Compliance Officer (compliance@hesinternational.eu). You can also contact the local compliance officer in case of any questions or requests.

You also have the right, at any time, to lodge a complaint about our processing of your personal information with a data protection authority. The relevant contact information can be found here: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

11. HOW... do you handle changes to this privacy notice?

This privacy statement will be reviewed by regularly and in addition may be reviewed from time to time to take account of, for example, changes to legislation, regulatory developments and organizational changes.

A new privacy statement will be provided to you when any substantial changes are made. We may also notify you in other ways from time to time about the processing of your personal information.

12. Update history

VERSION	REVISED BY	DESCRIPTION	REVISION DATE