HES - DATA PROTECTION IMPACT ASSESSMENT POLICY

1. Introduction

This is the data protection impact assessment policy (the "**DPIA Policy**") of HES International B.V. ("**HES**"). In this DPIA Policy, Personal Data means any information which relates to an identifiable living individual. This definition is very wide and captures almost any information (from a person's name to their mobile number) to the extent that it relates to a living individual who can be identified. In addition, Processing means collecting, storing, analysing, using, disclosing, archiving, deleting or doing absolutely anything else with Personal Data.

2. 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 an 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 its compliance program as it demonstrates that HES has carefully and properly considered any potential or actual risks presented by its Processing.

A DPIA is a key tool, both in ensuring compliance with the GDPR, but also in demonstrating that compliance. The DPIA framework is one important part of compliance with the wider 'accountability principle' imposed by the GDPR.

3. When is a DPIA required?

You (as the project leader in question or its delegate) should carry out a DPIA: (i) where a new information technology system or other arrangement (whether of a technical nature or otherwise) involving the Processing of Personal Data (a "**Processing System**") is to be implemented within or on behalf of HES, or (ii) a significant change is to be made to an existing Processing System.

Particular care should be taken where the Processing System may result in high risks for the privacy of the relevant data subjects. For example, where the Processing System:

- systematically monitors individuals;
- Processes Personal Data on a large sale;
- uses new or innovative technological solutions;
- deals with data of a highly personal or sensitive nature; or
- involves engaging a new supplier.

4. What should I do?

You should:

- ensure that full account is taken of the requirements of this DPIA Policy and the privacy rights of data subjects in the selection, design and implementation of the new or changed Processing System, including in particular:

  (a) keeping the Personal Data to be processed by the Processing System to the minimum level necessary for HES' business requirements; and

  (b) where Personal Data are to be processed and it is reasonably practicable and consistent for HES to do so, keeping data allowing the identification of data subjects separate from other elements of that Personal Data being processed, and effectively protected, so that the data subjects are not identifiable except where this is necessary for HES' business purposes; and

- consider the requirements of this DPIA Policy and the HES Privacy Policy for HES' Processing of Personal Data in that Processing System, and its implications for the privacy of data subjects. You should make sure to ensure that, following the implementation or change, the Processing System will comply with the principles set out in this DPIA Policy and the HES Privacy Policy in all respects and that its implementation will not result in high risks for the privacy of the relevant data subjects that cannot be mitigated.

5. Should a DPIA be executed?

Having considered the implications of this DPIA Policy and the HES Privacy Policy for HES' Processing of Personal Data in that Processing System, and its implications for the privacy of data subjects, you will need to decide if a DPIA should be executed.

If you are uncertain whether the principles of this DPIA Policy or the HES Privacy Policy apply, or believe the implementation of the new or changed Processing System may result in high risks for the privacy of the relevant data subjects, you should send the Local Compliance Officer a sufficiently detailed explanation of the proposed new Processing System or change to a Processing System, together with a summary of your assessment or queries, and your reasoning, by completing Part C of Annex 1 (an "**Initial Notice**").

On receiving the Initial Notice, the Local Compliance Officer will determine whether a DPIA is required and inform you of their decision. If the Local Compliance Officer determines that a DPIA is required, you should follow their instructions, including completing the DPIA form attached hereto in Part D of Annex 1 for the Local Compliance Officer's review (the "**DPIA Form**").

A new Processing System may not be implemented within or on behalf of HES, and no significant change may be made to an existing Processing System, unless the assessment referred to in sections 4 and 5 has been carried out and either:

- you (i) have considered the principles of this DPIA Policy and the HES Privacy Policy and believe they will be met in all respects and (ii) do not believe the implementation of the new or changed Processing System will result in high risks for the privacy of the relevant data subjects; or
- you have sent the Local Compliance Officer an Initial Notice and they have informed you that a full DPIA is not required; or
- you have conducted a full DPIA under the instruction of the Local Compliance Officer and the Local Compliance Officer has informed you that the new or changed Processing System and its implementation can go ahead.

6. Your obligations under the policy

We adhere to our data protection and privacy obligations, and take these very seriously. In the course of your duties with us, you are required to do the same. Failure to fulfil these duties and/or follow this Policy may constitute a disciplinary offence, and may result in dismissal.

7. Queries

If you have any queries about this Policy or are in doubt as to its requirements, please contact the Deputy Chief Compliance Officer (compliance@hesinternational.eu).

ANNEX 1

Template Data Privacy Impact Assessment Form

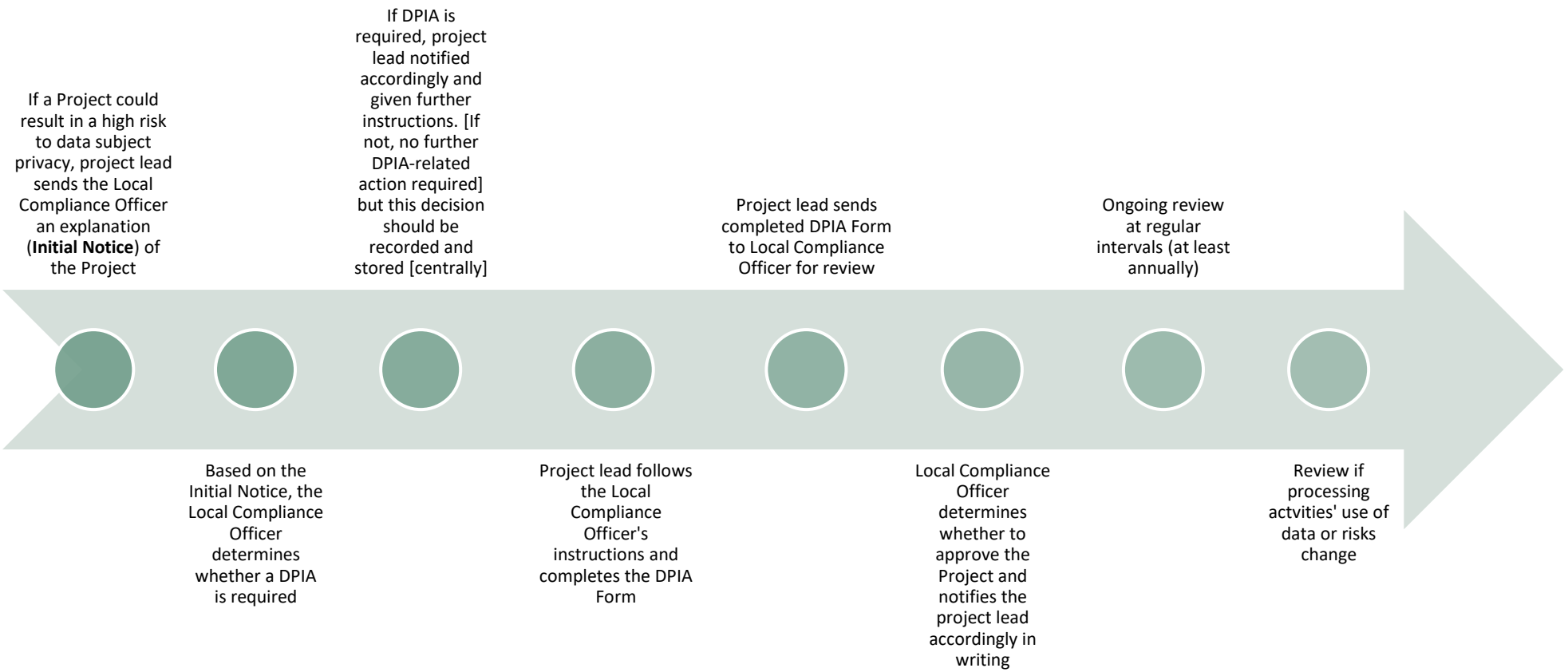
Part A: Introduction

Defined terms used in this Annex 1 can be found at Part E (*Glossary*) attached hereto.

Part B provides an overview diagram of the DPIA Process. Part C asks some preliminary questions in order to establish the nature of the Project and whether a DPIA is necessary ("the **Initial Notice**"). Part D is the DPIA form, and contains a series of questions about the proposed Project and its proposed use of personal information (the "**DPIA Form**").

Disclaimer: The DPIA Form does not provide for the situation when the controller must consult with the data protection supervisory authority. This should be led by the **Legal Department**.

Part B: Overview of the DPIA Process



Part C: Preliminary questions to determine whether a DPIA is necessary and if so, how to carry out that assessment ("Initial Notice")

General Project Information

Question	Answer
[*Relevant HES entity*] requesting/undertaking the Project	
Project lead details	Name: Role: Telephone: Email:
Will your project involve the Processing of Personal Data – if no, no further action required. Please send this form to the Local Compliance Officer for review and approval	
Please describe in as much detail as possible how your Project will involve the Processing of Personal Data?	
Will HES be Processing Personal Data as a Data Controller or Data Processor? In each case, explain why.	
What is the purpose of the Project?	
What are the benefits to HES?	
What are the potential benefits to other parties (including customers of HES and	

affected individuals, to the extent applicable)?	
Are there any documents that are relevant to the Project, such as a project proposal, that could be useful for the purposes of this DPIA – for example, setting out how personal data will be used? If so, please list them and append to this Form.	
By what date is the Project to be implemented?	

The Project and Personal Data

Question	Yes/No	Privacy Risk
Will the Project involve the collection of Personal Data about individuals?		Low-medium
Will the Project require individuals to provide information about themselves in order to provide the processing service, or is this voluntary?		Medium
How will the individuals be notified/informed?		Medium
Will Personal Data be disclosed to or stored within the HES organisation, or third parties, in a way not done previously?		Medium

Will the Personal Data be used for a new or different purpose?		Low-medium
Does the Project involve using new technology?		Medium-high
Will the Project result in the taking of decisions or the taking of actions against individuals in ways which could have a significant effect on them (profiling them for example)?		High
Will the Project involve any automated decision-making processes or the profiling of individuals?		High
Will the Project involve large scale Processing of Personal Data?		Medium-High
Will the Project involve large scale Processing of special category or criminal conviction and offence data?		High
Will there be cross-border Processing?		High

Summary

Question	Y/N
On the basis of the information and answers given above, does it appear that	

the Processing of Personal Data is likely to create high risks to data subjects or constitute a risky processing activity?	
If the answer to the question above is no, please detail the reasons for this conclusion here and return this form to the Local Compliance Officer for approval.	
If the answer is yes, please continue to the next section.	

Part D: Data Privacy Impact Assessment Form ("DPIA Form")

#	Question	Answer
The Personal Data		
1.	What Personal Data will be collected? (please circle Y/N as appropriate)	Name: Y / N Address: Y / N Date of birth: Y / N Racial or ethnic origin: Y / N Marital status: Y / N Family and relationship information: Y / N Religion: Y / N Health information: Y / N Sexual orientation: Y / N Political views: Y / N Genetic information: Y / N Criminal conviction information: Y / N Physical characteristic information (height, weight, etc): Y / N Credit card/bank account number: Y / N Ownership information (cars, houses, apartments, personal possessions): Y / N Credit history: Y / N Social network information: Y / N Other (please specify): Y / N
2.	How is it collected?	
3.	What is the Processing activity?	
4.	Is this Processing necessary or could the activity be carried out in a different way?	

#	Question	Answer
5.	Could the Project still be undertaken successfully without collecting some or all of this Personal Data?	
6.	About whom might Personal Data be collected/Processed? (Please circle Y/N as appropriate)	Employees: Y / N Non-employees: Y / N If non-employees, please specify who (customers, vendors, other third parties, etc):
7.	For what specific purpose will the Personal Data be Processed (e.g. to operate a new bespoke employee benefits portal)? Describe in as much detail as possible why the information is being processed.	
8.	For how long will the Personal Data be stored?	
The Legal Basis		
9.	Will the Personal Data be Processed on the basis of data subject consent? If so, how is this consent obtained?	
10.	Will the Personal Data be Processed in performance of a contract with the relevant data subjects?	
11.	Will the Personal Data be Processed on the basis of a legitimate business interest of HES (e.g. internal HR administration)?	
12.	Will the Personal Data be Processed on the basis of another legal justification	

#	Question	Answer
	(see Part F for a list of lawful justifications)?	
The Information Flows		
13.	After Personal Data is collected from the data subjects, where is it stored?	
14.	Who will have access to the Personal Data?	
15.	Will reports be run requiring use and disclosure of the Personal Data?	
16.	Will the Personal Data be transferred to any non-HES entity? If so, which entity and for what purposes?	
17.	Will the Personal Data be transferred to any countries or accessed by anyone outside of the European Economic Area?	
18.	Has a Personal Data mapping exercise been undertaken?	
19.	If the answer to (18) is "Yes", please provide a Personal Data map illustrating the flows of Personal Data involved in this Project. (noting personal data type, entities between which it is shared, locations of those entities and storage locations)	

#	Question	Answer
20.	How long will the Personal Data be kept for?	
Consultation Requirements		
21.	Who will you consult internally regarding the privacy and security risks associated with the Project?	
22.	Have you sought the advice of the local compliance officer, Deputy Chief Compliance Officer or Legal Department?	
23.	Do any works councils or other employee bodies need to be consulted (where HR/Employee data is involved)?	
24.	If there are cross-border transfers, does sign off need to be detailed from another jurisdiction?	
25.	If the answers to (23) or (24) above are "Yes", have you undertaken the proper consultation with the relevant parties? Please confirm here, and detail the consultations, with whom, and dates.	
Identifying Risks		
26.	Based on the questions above, what specific privacy issues have you identified, if any? E.g. risk that Personal Data is accessed by an unauthorised person, for example: • risk that the security of the data is compromised	

#	Question	Answer
	• risk that the individuals would object to the processing if informed • risk that the accuracy of the data is not maintained • risk that personal data is retained for longer than is necessary	
27.	What is the specific harm that such risks would pose to individuals (e.g. risk that Personal Data is stolen, resulting in relevant individuals being subjected to fraud and identity theft)?	
28.	Is there a specific compliance risk?	
29.	Is there a broader organisational risk (e.g. large penalties as a result of the breach and consequent adverse media coverage)?	
Steps and measures to safeguard, secure and protect the Personal Data		
30.	In respect of each risk identified above, what measures will be in place to secure and protect the Personal Data (e.g. encryption, multi-factor authentication)?	
31.	In respect of each risk identified above, how will we facilitate the exercise of	

#	Question	Answer
	data subject rights (for example, the right to access)?	
32.	How will appropriate information be communicated to the data subjects about the Project and associated privacy risks if necessary?	
33.	Will these actions eliminate the risk altogether, or simply reduce it?	
34.	Taking into account the identified risks and proposed solutions to mitigate those risks, is the final impact on the privacy rights of data subjects considered to be acceptable in light of the aims and benefits of the Project?	
Incorporate Findings and measures to eliminate/mitigate identified risks		
35.	How will these findings be incorporated into the Project?	
36.	Whose responsibility will it be to ensure the findings are properly integrated?	
37.	By when?	
38.	What is the process for data subjects who wish to discuss their privacy-related concerns in respect of the Project?	

Summary

Question	Y/N
Are the identified risks eliminated, reduced or accepted?	
If no, the processing must not commence until the DPIA has been escalated to [•] and suitable measures can be put in place.	

Sign off and approval/rejection	
Project Lead	
Name	
Job Title	
Signature	
Date	
Compliance Team Representative (if applicable)	
Name	
Job Title	
Signature	
Date	

Local Compliance Officer Determination	
Name	
Date	
Response	
Explanation (if applicable)	

Signature	

Part E

Glossary

Term	Definition
GDPR:	The General Personal Data Protection Regulation, which comes into force on 25 May 2018. The GDPR applies only to Personal Data – it does not include Personal Data relating to businesses and other non-living persons.
Data Controller:	The company which determines the purposes and means of Processing Personal Data.
Data Processor:	The company which Processes Personal Data on behalf of the Controller.
Local Compliance Officer	The person within the HES entity responsible for Data Privacy Impact Assessments.
Personal Data:	All information relating to identifiable individuals. Examples of Personal Data include:
	A. Name (such as full name, maiden name, or alias).
	B. Personal identification number (such as national insurance number, passport number, driver's license number, and financial account or credit card number).
	C. Address information (such as street address or email address).
	D. Asset information (such as Internet Protocol (IP) or Media Access Control (MAC) address).
	E. Telephone numbers (including mobile phone numbers).
	F. Personal characteristics, including photographic image (e.g. of face), x-rays, fingerprints, or other biometric image / template Personal Data (e.g. retina scan, voice signature, facial geometry).
	G. Information identifying personally owned property (such as vehicle registration number and related information).

	H. Information about an individual that is linked or linkable to one of the above; (e.g., date of birth, place of birth, race, religion, activities, geographical indicators, employment information, medical information, education information, financial information).
	I. Seemingly trivial information, such as the fact that an individual sent an email at a particular time, or the fact that an individual is an employee of a HES client (or other organisation).
	J. Opinions about an individual (such as opinions expressed in a reference or appraisal).
Processing:	Almost all operations carried out in relation to Personal Data, including:
	A. Collection, storage and recording;
	B. Organisation and structuring;
	C. Adaptation and alteration;
	D. Retrieval, consultation and use;
	E. Disclosure and dissemination;
	F. Alignment and combination; and
	G. Restriction, erasure and destruction.

Part F

List of Lawful Justifications for Processing

- **The individual whom the Personal Data is about has consented to the Processing.**
    - Consent must be express, informed and freely given. An individual must also be able to withdraw their consent. For more information on consent, please see the HES Privacy Policy.
- **The Processing is necessary:**
    - in relation to a contract which the individual has entered into; or
    - because the individual has asked for something to be done so they can enter into a contract.
- **The Processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).**
    - For example, data needs to be retained in order to comply with regulatory requirements, financial reporting requirements or anti-bribery and corruption law.
- **The Processing is necessary to protect the individual's "vital interests".**
    - This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital treating them after a serious road accident.
- **The Processing is in accordance with the "legitimate interests" condition.**
    - Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
    - It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
    - There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to: (i) identify a legitimate interest; (ii) show that the processing is necessary to achieve it; and (iii) balance it against the individual's interests, rights and freedoms.
    - The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits. The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.