SHV Privacy Code for Employee Data

(*Binding Corporate Rules* for the transfer of personal data
outside the EEA under Article 47 GDPR)

Introduction

SHV has committed itself to the protection of personal data it processes of its employees, customers, suppliers, business partners and other individuals in the SHV Business Support Framework and the SHV Policies & Guidelines.

This SHV Privacy Code for Employee Data indicates how SHV when processing personal data of its employees as a controller protects personal data subject to EEA data protection laws when transferred in the context of its business activities as a multinational corporation with operations, ranging from industrial services (ERIKS), cash and carry wholesale (Makro), heavy lifting and transport solutions (Mammoet), provision of private equity (NPM Capital), global distribution of off-grid energy such as LPG or LNG and activities in the area of sustainable fuels and renewable energy solutions (SHV Energy) to animal nutrition and fish feed (Nutreco).

This SHV Privacy Code for Employee Data constitutes *Binding Corporate Rules* for the transfer of personal data to a third country outside the EEA under Article 47 GDPR and is legally binding and shall apply to and be enforced by SHV Holdings and its Group Companies, including Employees.

For the rules applicable to customer, supplier and business partner data, please refer to the SHV Privacy Code for Customer, Supplier and Business Partner Data.

Capitalized terms that are not defined in this Privacy Code have the meanings given to them in the EU General Data Protection Regulation (**GDPR**).

Article 1 – Scope, Applicability and Implementation

Scope

1.1 This Code applies to the Processing by SHV as a Controller of Personal Data of Employees and their Dependents in the context of Employees' working relationship with SHV, where such Personal Data is subject to EEA Data Protection Laws or was subject to EEA Data Protection Laws prior to the Transfer of such Personal Data to a Group Company outside of the EEA (**Employee Data**). Any Processing of Personal Data of Employees and their Dependents by Group Companies outside the EEA that has not been subject to EEA Data Protection Law, shall at least be compliant with applicable local law and the security and governance provisions of this Code. For the avoidance of doubt, this Code does not address the Processing of Employee Data by participations of NPM Capital N.V.

This Code covers all types of Employee Data which SHV Processes in the context of its business activities and employment relationships, as detailed in **Annex 2**.

Electronic and paper-based Processing	1.2	This Code applies to the Processing of Employee Data by electronic means and in systematically accessible paper-based filing systems.
Sub-policies and notices	1.3	SHV may supplement this Code through sub-policies, guidelines or notices that are consistent with this Code.
Binding effect, accountability for compliance	1.4	This Code is legally binding and shall apply to and be enforced by SHV Holdings and its Group Companies, including Employees. The Responsible Executives will be accountable for compliance with this Code.
Effective Date	1.5	This Code has been adopted by the Executive Board of Directors of SHV Holdings. It has entered into force as of 1 April 2024 (**Effective Date**). The Code (including a list of the Group Companies= link) will be published on the SHV Holdings intranet and communicated by Group Companies to their Employees (e.g., on Group Company intranet, as applicable). It will further be made available to Employees upon request.
Code supersedes prior policies	1.6	This Code will supersede all SHV privacy policies and notices that exist on the Effective Date to the extent they are in contradiction with this Code.

Article 2 – Purposes for Processing Employee Data

Lawful Processing 2.1 Employee Data shall be Processed lawfully. Lawful Processing means that SHV will not Process Employee Data, unless one of the following conditions applies:

(i) SHV needs to Process Employee Data to:
  (a) perform, or take steps with a view to enter into, a contract with the relevant Employee;
  (b) comply with a legal obligation to which SHV is subject;
  (c) protect the vital interests of the Employee;

(ii) SHV needs to carry out such Processing to pursue SHV's legitimate interests, and these interests do not prejudice the interests or fundamental rights and freedoms of the Employee concerned; or

(iii) the Employee concerned has consented to the Processing, by providing a freely given, specific, informed and unambiguous indication of the Employee's wishes by a clear affirmative action;

(iv) In circumstances permitted by EEA Data Protection Law.

SHV will not use Employee Data for new purposes without following our internal procedures to verify that such Processing can take place lawfully.

Legitimate Business Purposes 2.2 SHV Processes Employee Data for the business purposes set out in **Annex 2** (**Business Purposes**) but remains subject to any applicable requirements and restrictions under EEA Data Protection Law.

Where there is a question whether a Processing of Employee Data can be based on a Business Purpose, the relevant Group Privacy Officer will be consulted before the Processing takes place.

Employee consent

2.3 Employee consent generally cannot be used as a legitimate basis for Processing Employee Data. One of the Business Purposes will have to exist for any Processing of Employee Data. If applicable law so requires, in addition to having a Business Purpose for the relevant Processing, SHV shall also seek Employee consent for the Processing. If none of the Business Purposes apply, SHV may request Employee consent for Processing Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee.

A request for Employee consent will require the consultation of the relevant Group Privacy Officer prior to seeking consent.

Consent process

2.4 When seeking Employee consent, SHV shall inform the Employee:

(i) of the purposes of the Processing for which consent is requested;
(ii) which Group Company is responsible for the Processing;
(iii) of the potential consequences for the Employee of the Processing;
(iv) that he or she is free to withdraw consent at any time without consequence to his or her employment relationship; and
(v) that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal.

The Employee may deny or withdraw consent at any time. Upon withdrawal of consent, SHV will discontinue the Processing as soon as reasonably practical. The withdrawal of consent shall not affect (i) the lawfulness of the Processing based on such consent before its withdrawal; and (ii) the lawfulness of Processing of the relevant Employee Data after withdrawal, for other Processing Purposes not based on consent.

Limitations on Processing Data of Dependants of Employees

2.5 SHV will Process Data of Dependants of an Employee if:

(i) the Data were provided with the consent of the Employee or the Dependant;
(ii) Processing of the Data is reasonably necessary for the performance of a contract with the Employee or for managing the Employment-at-will relationship; or
(iii) the Processing is required or permitted by applicable law.

Article 3 – Use for Other Purposes

Use of Data for Secondary Purposes

3.1 Employee Data may be Processed for a purpose other than the Business Purpose(s) for which the Employee Data was originally collected, only if the additional purpose is compatible with the relevant Business Purpose(s), taking into account the link between the original and additional purpose, the context in which the Employee Data is collected, the nature of the relevant Employee Data and the implementation of appropriate safeguards set out below (**Secondary Purpose**). When assessing if Employee Data can be Processed for a Secondary Purpose, the relevant Group Privacy Officer will be consulted.

Depending on the sensitivity of the relevant Employee Data and the possible consequences for the Employee, the Processing of Employee Data for the Secondary Purpose may require additional safeguarding measures (such as

limiting access to the Employee Data or taking additional security measures) to mitigate the consequences. If the consequences cannot be appropriately mitigated, SHV may need to provide the Employee an opt-out opportunity, or obtain the Employee's consent.

Examples of Permitted Uses for Secondary Purposes

3.2 To the extent not already covered in Article 2.1, and subject to the compatibility assessment referred to in Article 3.1, below are a number of examples of Processing for Secondary Purposes that may be permissible:

(i) anonymization or pseudonymization of the Employee Data;
(ii) internal audits or investigations;
(iii) implementation of business controls and operational efficiency;
(iv) IT systems and infrastructure related Processing such as for maintenance, support, life-cycle management, and security (including resilience and incident management);
(v) for the purposes of public interest, scientific or historical research purposes or statistical purposes, including the transfer of the Employee Data to an archive for these purposes;
(vi) dispute resolution;
(vii) legal or business consulting; or
(viii) insurance purposes.

The Business Purposes and Secondary Purposes together constitute the **Processing Purposes**.

Article 4 – Purposes for Processing Special Categories of Data

Specific purposes for Processing Special Categories of Data

4.1 SHV will Process Special Categories of Data only to the extent necessary to serve one (or more) of the purposes specified in **Annex 2** or as otherwise provided by EEA law.

Lawful Processing of Special Categories of Data

4.2 In addition to the specific purposes listed in Article 4.1 above, Special Categories of Data shall be Processed lawfully. Lawful Processing means that SHV will not Process Special Categories of Data, unless one of the following conditions applies:

(i) when necessary for the performance of a task carried out to comply with or authorised by law;
(ii) for the establishment, exercise or defence of a legal claim;
(iii) to protect a vital interest of an Employee, but only where it is impossible to obtain the Employee's consent first;
(iv) to the extent necessary for reasons of substantial public interest;
(v) where the Special Categories of Data have manifestly been made public by the Employee (e.g., via SHV social media channels); or
(vi) archiving for the purposes of public interest, scientific or historical research purposes or statistical purposes.

Employee consent for Processing Special Categories of Data	4.3	Employee consent generally cannot be used as a legitimate basis for Processing Special Categories of Data. One of the grounds listed in Article 4.1 or 4.2 must exist for any Processing of Special Categories of Data. If applicable law so requires, in addition to having one of the grounds listed in Article 4.1 or 4.2 for the relevant Processing, SHV shall also seek Employee consent for the Processing. If none of the grounds listed in Article 4.1 or 4.2 applies, SHV may request Employee consent for Processing Special Categories of Data, but only if the Processing has no foreseeable adverse consequences for the Employee (e.g., Employee diversity programs or networks, research, product development, selection of candidates in hiring or management development processes). Article 2.4 will apply to the granting, denial, or withdrawal of Employee consent.
Prior consultation of Group Privacy Officer	4.4	Where Special Categories of Data are Processed based on a requirement of law other than the law applicable to the Processing, or based on the consent of the Employee, the Processing will require the prior consultation of the relevant Group Privacy Officer.
Use of Special Categories of Data for Secondary Purposes	4.5	Special Categories of Data of Employees or Dependants may be Processed for Secondary Purposes in accordance with Articles 3 and 4.2.

Article 5 – Quantity and Quality of Data

No Excessive Data	5.1	SHV shall limit the Processing of Employee Data to the Data that is necessary and adequate for and relevant to the applicable Processing Purpose. SHV shall take steps to delete or otherwise destroy Employee Data that is not required for the applicable Processing Purpose.
Storage period	5.2	SHV specifies – e.g., in a policy, statement, records retention schedule or in new systems via 'privacy by design' – a time period for which certain categories of Employee Data may be kept, which means not for longer than necessary for the applicable Processing Purpose. Promptly after the applicable storage period has ended, the Data shall be: (i) securely deleted or destroyed; or (ii) anonymised.
Quality of Data	5.3	Employee Data will be accurate, complete, and kept up to date to the extent necessary for the applicable Processing Purpose. SHV shall take reasonable steps to rectify or erase Employee Data that is inaccurate without delay.
'Self-service'	5.4	Where SHV requires an Employee to update his or her own Employee Data, SHV shall remind him or her at least once a year to do so.

'Privacy by Design and Default'

5.5 SHV shall implement appropriate technical and organizational measures which are designed to implement the data protection principles of, and to facilitate compliance with, this Code in practice, consistent with privacy by design and privacy by default principles under EEA Data Protection Law, both at the time of determination of the means for Processing and at the time of the Processing itself, and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Employees.

Article 6 – Employee Information Requirements

Information requirements

6.1 At the time when Employee Data is obtained, or prior to Processing Employee Data for a Secondary Purpose, SHV shall inform Employees through a privacy policy or notice of the following:

(i) the nature and categories of Employee Data Processed;
(ii) which Group Company or Group Companies are solely or jointly responsible for the Processing;
(iii) the contact details of the relevant Group Privacy Officer or designated central point of contact for data privacy matters within SHV; and
(iv) the Processing Purposes for which their Employee Data is Processed.

SHV will also inform Employees about other relevant information, such as:

(i) the legal basis for the Processing of their Employee Data and, if the Processing is based on the legitimate interests of SHV, of the legitimate interests pursued by SHV;
(ii) the categories of Third Parties to which the Employee Data is disclosed (if any);
(iii) whether such Third Party is covered by an Adequacy Decision, and if not, information on the data transfer mechanism as referred to in Article 11.6 as well as the means to get a copy thereof, or access thereto;
(iv) the retention period of the Employee Data or the criteria to determine the retention period;
(v) the Employee's rights under this Code and how these rights may be exercised, including the right to obtain compensation;
(vi) the right to lodge a complaint with a Supervisory Authority;
(vii) about the existence of automated decision making, including profiling, and about the logic behind and envisaged consequences of this automated decision making; and
(viii) if the Employee Data were not collected from the Employee him or herself, the source from which the Employee Data originate, including whether the Employee Data came from a public source.

Employee Data not collected from the Employee

6.2 Where Employee Data has not been obtained directly from the Employee, SHV shall provide the Employee with the information as set out in Article 6.1:

(i) within reasonable period after obtaining Employee Data but at the latest within one month, having regard to specific circumstances of the Employee Data Processed;

(ii) if Employee Data is used for communication with Employee, at the latest at the time of the first communication with the Employee;

(iii) if a disclosure to another recipient is envisaged, at the latest when Employee Data is first disclosed.

Exceptions

6.3 The requirements of Articles 6.1 and 6.2 may be inapplicable if:

(i) the Employee already has the information as set out in Article 6.1;

(ii) it would be impossible or would involve a disproportionate effort to provide the information to Employees, in which case SHV will take additional measures to mitigate potential negative consequences for the Employee, such as those described in Article 3.1;

(iii) obtaining Employee Data is expressly laid down in applicable EEA law; or

(iv) the Employee Data must remain confidential subject to an obligation of professional secrecy regulated by applicable local law, including a statutory obligation of secrecy.

Article 7 – Employee Rights

Right of access

7.1 Every Employee has the right to request confirmation whether his or her Employee Data is Processed, request a copy thereof as well as request access to the information listed in Article 6.1 or 6.2

Right to rectification, deletion, and restriction

7.2 If the Employee Data is incorrect, incomplete, or not Processed in compliance with EEA Data Protection Law or this Code, the Employee has the right to have his or her Employee Data:

(i) **rectified or completed**, if such Employee Data is incorrect or incomplete;

(ii) **deleted**, if such Employee Data is not Processed in compliance with EEA Data Protection Law or this Code. In case the Employee Data has been made public by SHV, and the Employee is entitled to deletion of the Employee Data, in addition to deleting the relevant Employee Data, SHV shall, taking account of available technology and the cost of implementation, take reasonable steps to inform Third Parties that are Processing the relevant Employee Data or linking to the relevant Employee Data, that the Employee has requested the deletion of the Employee Data; or

(iii) **restricted** from other Processing than storage, pending verification in case the accuracy of such Employee Data is contested or if the Employee objects to such Processing under Article 7.3(i), or where the Processing is unlawful or no longer needed, but the Employee prefers

restriction to erasure of the Employee Data. SHV will only Process the restricted Employee Data with the Employee's consent or as permitted by EEA Data Protection Law. SHV will inform the Employee before the restriction is lifted.

SHV shall communicate any rectification, deletion or restriction in accordance with the rights sub (i)-(iii) above, to any Third Party to whom the relevant Employee Data has been disclosed, unless this proves impossible or involves disproportionate effort. SHV will inform the Employee about those recipients upon request.

Right to object 7.3 The Employee has the right to object to:

(i) the Processing of his or her Employee Data on grounds relating to his or her particular situation, unless SHV can demonstrate prevailing compelling legitimate grounds for the Processing; and

(ii) receiving marketing communications.

Restrictions to rights of Employees 7.4 The rights of Employees set out in Articles 7.1 - 7.3 are subject to any applicable exceptions provided under EEA Data Protection Law. Applying exceptions requires the prior consultation of the relevant Group Privacy Officer. Depending on the relevant right of the Employee, exceptions may be available in cases where:

(i) the Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of SHV;

(ii) the Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;

(iii) the Processing is necessary for exercising the right of freedom of expression and information;

(iv) for dispute resolution purposes;

(v) the exercise of the rights by the Employee adversely affects the rights and freedoms of others; or

(vi) in case a specific restriction of the rights of Employees applies under applicable EEA law.

Procedure 7.5 The Employee may send his or her request to the relevant Group Privacy Officer. If SHV Processes a large quantity of Data relating to an Employee, prior to fulfilling the request of the Employee, SHV may require the Employee to:

(i) specify the categories of Employee Data to which he or she is seeking access;

(ii) specify to the extent reasonably possible the data system in which the Employee Data is likely to be stored;

(iii) specify to the extent reasonably possible the circumstances in which SHV obtained the Employee Data;

(iv) provide proof of his or her identity when SHV has reasonable doubts concerning such identity, or to provide additional information enabling his or her identification; and

(v) in the case of a request for rectification, deletion, or restriction, specify the reasons why the Employee Data is incorrect, incomplete, or not Processed in accordance with applicable law or this Code.

Response period

7.6 Within one month of SHV receiving the request and any information necessary under Article 7.5, the Group Privacy Officer shall inform the Employee in writing either (i) of SHV's position regarding the request and any action SHV has taken or will take in response or (ii) the ultimate date on which he or she will be informed of SHV's position. This date will be no later than two months after the original one month period. SHV shall explain the reasons of this delay.

Complaint

7.7 An Employee may file a complaint in accordance with Article 17.3 and/or file a complaint or claim with the SAs or the courts in accordance with Article 18 if:

(i) the response to the request is unsatisfactory to the Employee (e.g., the request is denied);

(ii) the Employee has not received a response as required by Article 7.6; or

(iii) the time period provided to the Employee in accordance with Article 7.6 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response.

Denial of requests

7.8 SHV may deny an Employee's request if:

(i) the request does not meet the requirements of Articles 7.1 – 7.3 or meets the requirement of Article 7.4;

(ii) the request is not sufficiently specific (and the Employee was given the opportunity to specify his or her request);

(iii) the identity of the relevant Employee cannot be established by reasonable means, including additional information provided by the Employee; or

(iv) SHV can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character. A time interval between requests of 6 months or less shall generally be deemed to be an unreasonable time interval;

(v) the Processing is required by or allowed for the performance of a task carried out to comply with a legal obligation of SHV;

(vi) the Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;

(vii) the Processing is necessary for exercising the right of freedom of expression and information;

(viii) for dispute resolution purposes;

(ix) in so far as the request violates the rights and freedoms of others; or

(x) in case a specific restriction of the rights of Employees applies under applicable EEA law.

The right of access set out in Article 7.1 can only be denied under, and for the duration of, the circumstances listed in items (viii), (ix), and (x) above.

No requirement to Process identifying information	7.9	SHV is not obliged to Process additional information to be able to identify the Employee for the sole purpose of facilitating the rights of Employees under this Article 7.

Article 8 – Security and Confidentiality Requirements

Data security	8.1	SHV shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Employees, take appropriate technical and organisational measures to protect Employee Data from misuse or accidental, unlawful, or unauthorised destruction, loss, alteration, disclosure, acquisition, access or other Processing. To achieve this, SHV has developed and implemented the SHV Information Security Program and other sub-policies relating to the protection of Employee Data.
Staff access	8.2	Staff will be authorised to access Employee Data as necessary to serve the applicable Processing Purpose and to perform their job as instructed by SHV.
Confidentiality obligations	8.3	Staff who access Employee Data will meet their confidentiality obligations.
Data Security Breach notification requirement	8.4	Data Security Breaches are reported to the SHV Privacy Function in accordance with SHV's established incident response procedures. SHV shall document any Data Security Breach, comprising the facts relating to the Data Security Breach, its effects and the remedial actions taken, which documentation will be made available to any Competent SA upon request. SHV shall notify the appropriate Supervisory Authority(s) of a Data Security Breach without undue delay, and where feasible within 72 hours after becoming aware of it, unless the Data Security Breach is unlikely to result in a risk to the rights and freedoms of Employees. In addition, if a Data Security Breach is likely to result in a high risk to the rights and freedoms of Employees, SHV will notify Employees of a Data Security Breach without undue delay, following its determination that a Data Security Breach has occurred. Notifications may be delayed as instructed by law enforcement, where it determines that such notifications would impede a (criminal) investigation or cause damage to national security. SHV shall respond promptly to inquiries of affected Employees relating to such Data Security Breach.

Article 9 – Intentionally left blank

[●]

Article 10 – Automated Decision Making and Profiling

Automated decisions

10.1 Employees have the right not to be subject to a decision based solely on automated decision-making, including profiling, which produces legal (or similar significant) effects on him or her. This restriction will not apply if:

(i) the use of automated tools is authorized by EEA law;

(ii) the decision is necessary for purposes of (a) entering into or performing a contract between the Employee and SHV or (b) managing the Employment-at-will relationship between the Employee and SHV, provided the underlying request leading to a decision by SHV was made by the Employee (e.g., where automated tools are used to filter job applications); or

(iii) the Employee has given his or her explicit consent.

Special Categories of Data

10.2 SHV will only Process Special Categories of Data for automated decision-making purposes in the case referred to in Article 10.1(iii) or Article 4.2(iv) and SHV has taken suitable measures set out in Article 10.3.

Suitable measures

10.3 In the cases referred to in Article 10.1(ii) and (iii), SHV shall take suitable measures to safeguard the legitimate interests of the Employee, including at least the right for the Employee to obtain human intervention and to express his or her point of view.

Article 11 – Transfer of Employee Data to Third Parties

Transfer to Third Parties

11.1 This Article sets forth requirements concerning the transfer of Employee Data from SHV to a Third Party. Note that a transfer of Employee Data will include situations in which SHV discloses Employee Data to Third Parties (e.g., in the context of corporate due diligence) or where SHV provides remote access to Employee Data to a Third Party.

Third Party Controllers and Third Party Processors

11.2 There will be two categories of Third Parties:

(i) **Third Party Controllers**: these are Third Parties that Process Employee Data and determine the purposes and means of the Processing (e.g., government authorities or service providers that provide services directly to Employees); and

(ii) **Third Party Processors**: these are Third Parties that Process Employee Data solely on behalf of SHV and at its direction (e.g., Third Parties that Process Employee salaries on behalf of SHV).

Transfer for applicable Processing Purposes only

11.3 SHV shall transfer Employee Data to a Third Party to the extent necessary to serve the applicable Processing Purpose for which the Employee Data is Processed.

Third Party Controllers

11.4 Third Party Controllers (other than government agencies) may Process Employee Data transferred by SHV only if they have validly entered into a written or electronic contract with SHV. In such contract, SHV shall seek to contractually protect the privacy interests of its Employees when Employee Data is Processed by Third Party Controllers. All such contracts shall be drafted consistent with appropriate contracting guidelines. This provision does not apply in case of incidental transfers of SHV Employee Data to a Third Party Controller, such as, when a reference is provided for an Employee or in case of sending details for a hotel booking.

Third Party Processor contracts

11.5 Third Party Processors may Process Employee Data only if they have a written contract with SHV. The contract with a Third Party Processor will include the following provisions:

(i) the Third Party Processor shall Process Employee Data only in accordance with SHV's documented instructions and for the purposes authorised by SHV;

(ii) the Processor shall, and have persons it authorises to Process Employee Data, keep the Employee Data confidential;

(iii) the Processor shall take appropriate technical, physical and organisational security measures to protect the Employee Data;

(iv) the Third Party Processor shall not permit subcontractors and affiliates to Process Employee Data in connection with its obligations to SHV without (i) the prior specific or generic consent of SHV, and (ii) a validly entered into written contract between the Third Party Processor and the subcontractor, which imposes data protection obligations that shall be no less protective than those imposed on the Third Party Processor, and provided that the Third Party Processor remains liable to SHV for the performance of the subcontractors. In case SHV gives generic consent, the Third Party Processors shall provide notice to SHV of any changes in its subcontractors and will provide SHV the opportunity to object to such changes based on reasonable grounds;

(v) the Third Party Processor shall ensure that its subcontractors and affiliates abide by a level of data protection no less protective than the obligations as set out in the contract between the Third Party Processor and SHV;

(vi) SHV may review the security measures taken by the Third Party Processor and the Third Party Processor shall submit its relevant data processing facilities to audits and inspections by SHV, a Third Party on behalf of SHV or any relevant government authority. This may also be done by means of a statement issued by a qualified independent third party assessor certifying that the information processing facilities of the Third Party Processor used for the Processing of Employee Data comply with the requirements of the contract;

(vii) the Third Party Processor shall promptly inform SHV of any actual or suspected security breach involving Employee Data;

(viii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide SHV with all relevant information and assistance as requested by SHV regarding the security breach;

(ix) the Third Party Processor shall deal promptly and appropriately with (a) requests for information necessary to demonstrate compliance of the Third Party Processor with its obligations under the contract and will inform SHV if any instructions of SHV in this respect violate EEA Data Protection Law, (b) requests and complaints of Employees as instructed by SHV, and (c) requests for assistance of SHV as reasonably required to ensure compliance of the Processing of the Employee Data with EEA Data Protection Law; and

(x) at the choice of SHV, the Third Party Processor shall delete or return all Employee Data to SHV at the end of the provision of services relating to the Processing of Employee Data, and shall delete all copies of the Employee Data, unless storing the Employee Data is required by applicable EEA law.

Transfer of Employee Data to a Third Party in a country outside the EEA

11.6 SHV may transfer Employee Data to a Third Party Controller or Third Party Processor located outside the EEA if:

(i) the transfer is based on an Adequacy Decision;

(ii) in accordance with a data transfer mechanism that is recognized under EEA Data Protection Law as providing an adequate level of data protection; or

(iii) the transfer is subject to a derogation for specific situations under EEA Data Protection Law (i.e., the Processing is necessary for the conclusion or performance of a contract in the interest of the Employee, to protect a vital interest of an individual, for the establishment, exercise, or defence of a legal claim, or for important reasons of public interest (as recognized by the EEA law to which the Data Exporter is subject), or the Employee has given his or her explicit consent to the transfer, in accordance with Article 2.4).

A transfer based on Article 11.6 (iii) will require the prior consultation of the relevant Group Privacy Officer or Corporate Privacy Officer.

Prior to a transfer under (ii), SHV will conduct a Transfer Impact Assessment in accordance with Article 14.4.

Internal Processors

11.7 Internal Processors may Process Employee Data only if they have a validly entered into written or electronic contract with the Group Company being the Controller of the relevant Employee Data, which contract must in any event include the provisions set out in Article 11.5 above.

Article 12 – Restrictions under EEA law

Restrictions

12.1 Certain rights of Employees and obligations of SHV in this Code may in specific

under EEA law

cases be subject to restrictions provided by EEA law, as specified and applied in accordance with EEA Data Protection Law, such as to:

(i) prevent or investigate criminal offences (including cooperating with law enforcement);
(ii) enforce civil law claims; or
(iii) protect Employees or the rights or freedoms of others.

Applying such restrictions requires the prior consultation of the relevant Group Privacy Officer or Corporate Privacy Officer and will be documented.

Article 13 – Supervision and Compliance

SHV Privacy Function

13.1 SHV has established an SHV Privacy Function, which is coordinated by the Corporate Privacy Officer and consists of a global network of Group Privacy Officers and their respective network of Business Unit Privacy Officers, sufficient to direct compliance with this Code. Were required under EEA Data Protection Law, the Groups will appoint a DPO for their respective Group(s), Business Unit(s), or country organization(s). Such DPO(s) will be part of the SHV Privacy Function and will perform his/her statutory duties under EEA Data Protection Law. The DPO(s) report(s) on privacy compliance to the Board of Directors of the relevant Group or Group Company. Where a Group Privacy Officer or Business Unit Privacy Officer is also appointed DPO, he/she shall carry out his/her job responsibilities to the extent they do not conflict with his or her statutory position.

Corporate Privacy Officer

13.2 SHV Holdings shall appoint a Corporate Privacy Officer who is responsible for:

(i) supervising overall compliance with this Code within SHV;
(ii) coordinating, communicating and consulting with the Group Privacy Officers as described in this Code and on general data protection issues;
(iii) be available for requests for consultation, e.g., as described in Article 12.4;
(iv) providing an annual privacy compliance report to the Executive Board of Directors of SHV Holdings on data protection risks and compliance issues as described in Article 16.2;
(v) maintaining a fully updated list of the Group Companies and keep track and records of updates to this Code;
(vi) coordinating, in conjunction with the Group Privacy Officers and, if necessary, the relevant Business Unit Privacy Officers, compliance officers, the Legal Department and Audit Department, official investigations or inquiries into the Processing of Employee Data by a government authority;
(vii) dealing with conflicts between this Code and applicable law as described in Article 20;
(viii) advising on transfers as described in Articles 11.6 and 20.1;
(ix) keeping a record of any changes made to this Code as described in Article 21.1;

(x) monitoring the overall performance and periodic review of Data Protection Impact Assessments (DPIAs) within SHV;
(xi) monitoring the system of documentation, notification, and communication of Data Security Breaches within SHV; and
(xii) deciding on complaints as described in Article 17.3.

SHV Holdings Ethics and Compliance Committee

13.3 The Ethics and Compliance Committee of SHV Holdings shall ensure that a framework is in place for devising the data management processes, systems and tools to implement the overall framework for data protection management within SHV, such as:

(i) maintaining, updating and publishing this Code and related sub-policies;
(ii) a tool to collect, maintain and update information regarding the structure and functioning of all systems that Process Employee Data;
(iii) data privacy training and awareness for staff to comply with their responsibilities under this Code;
(iv) appropriate internal audit systems to monitor, audit and report compliance with this Code and enable SHV's internal audit department to verify and certify such compliance in line with the yearly SHV assurance process;
(v) procedures regarding data protection inquiries, concerns, and complaints; and
(vi) determining and updating appropriate sanctions for violations of this Code (e.g., disciplinary standards).

The SHV Holdings Ethics and Compliance Committee will also conduct the tasks of the Group Ethics and Compliance Committee as described in Article 13.5 in respect of SHV Holdings.

Group Privacy Officer

13.4 Each Group shall designate a Group Privacy Officer. A Group Privacy Officer may, in turn, establish a network of Business Unit Privacy Officers sufficient to direct compliance with this Code within their Group.
The Group Privacy Officer is responsible for the following tasks in respect of his or her Group:

(i) supervising, supporting and assessing compliance with this Code;
(ii) implementing and further developing (as applicable to his or her Group) the data management processes, systems and tools, devised by the Corporate Privacy Officer, the SHV Holdings Ethics and Compliance Committee and the Group Ethics and Compliance Committee to implement the framework for data protection management;
(iii) supporting and assessing overall data protection management compliance;
(iv) advising the Responsible Executive and the Corporate Privacy Officer on privacy risks and compliance issues;
(v) maintaining or ensuring access to an inventory of the system and information about the structure and functioning of all systems that Process Employee Data (as required by Article 14.2);
(vi) being available for requests for consultation as described in Article 3.1

and Article 12.4;

(vii) being available for requests, consultations or advice as described in Article 4.4 and Article 7;

(viii) providing information relevant to the annual privacy compliance report of the Corporate Privacy Officer (as required in Article 16);

(ix) assisting the Corporate Privacy Officer in the event of official investigations or inquiries by government authorities;

(x) authorising all appropriate privacy sub-policies;

(xi) directing that stored Data be deleted, destroyed, or anonymised as required by Article 5.2;

(xii) deciding on and notifying the Corporate Privacy Officer of complaints as described in Article 17;

(xiii) dealing with conflicts between this Code and applicable law as described in Article 20;

(xiv) advising on transfers as described in Articles 11.6 and 20.1; and

(xv) cooperating with the Corporate Privacy Officer, the other Group Privacy Officers, the Business Unit Privacy Officers (if applicable) and compliance officers to:

(a) ensure that the instructions, tools and training are in place to enable the Group to comply with this Code;

(b) share best practices for data protection management;

(c) ensure that data protection requirements are taken into account whenever new technology is implemented; and

(d) notify the Responsible Executive of the requirements in respect of the involvement of a Third Party Controller or Third Party Processor.

Group Ethics and Compliance Committee

13.5 The Ethics & Compliance Committee of a Group shall ensure that a framework is in place for devising the data management processes, systems and tools to implement the overall framework for data protection management within such Group, such as:

(i) developing, implementing and updating of local Employee data protection statements, policies and procedures;

(ii) maintaining, updating and publishing of this Code and establishing, maintaining, updating and publishing of related sub-policies;

(iii) creating, maintaining and updating of information regarding the structure and functioning of all systems that Process Employee Data (as required by Article 14);

(iv) developing, implementing and updating of data protection training and awareness programs;

(v) monitoring, auditing and reporting on compliance with this Code to the management board of the Group;

(vi) collecting, investigating and resolving privacy inquiries, concerns and complaints; and

(vii) determining and updating appropriate sanctions for violations of this Code (e.g. disciplinary standards).

Responsible Executive

13.6 The Responsible Executive will be accountable for the implementation of effective data protection management, the integration of effective data protection into business practice and that adequate resources and budget are available.

The Responsible Executive will specifically be accountable for:

(i) ensuring overall data protection management compliance, also during and following organisational restructuring, outsourcing, mergers and acquisitions and divestures;
(ii) implementing the data management processes, systems and tools, devised by the Corporate Privacy Officer and the Group Privacy Officer to implement the framework for data protection management;
(iii) ensuring that the data protection management processes and systems are maintained up to date against changing circumstances and legal and regulatory requirements;
(iv) ensuring and monitoring on-going compliance of Third Parties with the requirements of this Code in case Employee Data is transferred to a Third Party;
(v) ensuring that relevant Employees follow the prescribed data protection training courses; and
(vi) directing that stored Data be deleted, destroyed, or anonymised as required by Article 5.2.

The Responsible Executive will be responsible for:

(i) appointing a Group Privacy Officer;
(ii) consulting with the Corporate Privacy Officer in all cases where there is a conflict between applicable law and this Code as described in Article 20.1; and
(iii) informing the Corporate Privacy Officer if any new legal requirement interferes with SHV's ability to comply with this Code as required by Article 20.2.

Default Group 1Privacy Officer

13.7 If at any moment in time there is no Group Privacy Officer designated for a Group, the designated Ethics & Compliance officer for the relevant Group will be responsible for supervising compliance with this Code. A privacy officer conducting the tasks of the Group Privacy Officer as described in Article 13.4 in respect of SHV Holdings shall be appointed by SHV Holdings.

Article 14 – Policies and Procedures

Policies and procedures

14.1 SHV shall develop and implement sub-policies and procedures to comply with this Code.

Records of Processing Activities

14.2 SHV will maintain Records of Processing Activities. A copy will be provided to any Competent SA upon request.

Data Protection

14.3 SHV shall conduct a Data Protection Impact Assessment (DPIA) for Processing

Impact Assessment (DPIA)		operations that are likely to result in a high risk to the rights and freedoms of Employees. The DPIA will be performed prior to implementation of the envisaged IT system or Processing. Where a DPIA indicates that the Processing would result in a high risk in the absence of measures taken by SHV to mitigate the risk, the competent SA shall be consulted prior to Processing.
Transfer Impact Assessment	14.4	SHV will perform a Transfer Impact Assessment prior to a Transfer of Employee Data under this Code and maintain it for the duration of the Transfer. Where a Transfer Impact Assessment shows gap(s) in protection for Employees under this Code, SHV will implement supplementary measures, such as contractual, technical, or organizational safeguards, including measures applied during transmission and to the Processing of Employee Data in the country of destination to ensure compliance with the Code. Supplementary measures are not required in relation to laws and practices applicable to the Data Importer that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR. The Transfer shall not take place or will be suspended where: (i) compliance with this Code cannot be assured, (ii) no appropriate supplementary measures can be taken, or (iii) so instructed by any Competent SA. In case of suspension, the Data Exporter may choose to terminate the Transfer. In case of termination of a Transfer, including where a Data Importer ceases to be bound by this Code, the Data Importer must – at the Data Exporter's option – return or delete the Employee Data it received under this Code. SHV will conduct and document the Transfer Impact Assessment with the involvement of SHV Holdings and the Group Privacy Officer and will notify the Data Exporter and Data Importer thereof. SHV will make the Transfer Impact Assessment available to all Group Companies, and to any Competent SA upon request.

Article 15 – Training

Staff training	15.1	SHV shall provide training on the obligations and principles laid down in this Code and related confidentiality obligations to Staff who have permanent or regular access to Employee Data, who are involved in the collection of data or in the development of tools used to Process Employee Data.

Article 16 – Monitoring and Auditing Compliance

Audits

16.1 SHV Internal Audit or Group Internal Audit shall regularly audit business processes and procedures that involve the Processing of Employee Data for compliance with all aspects of this Code, including methods of ensuring that corrective actions will take place. The audits may be carried out in the course of the regular activities of SHV Internal Audit or Group Internal Audit or at the request of the Corporate Privacy Officer or the relevant Group Privacy Officer. The Corporate Privacy Officer may request to have an audit as specified in this Article 16.1 conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality will be observed when conducting an audit. The Responsible Executive, the Corporate Privacy Officer and the relevant Group Privacy Officer will be informed of the results of the audits. SHV shall provide a copy of the audit results to any Competent SA upon request.

Annual privacy report

16.2 The Corporate Privacy Officer shall produce an annual privacy compliance report for the Executive Board of Directors of SHV Holdings on compliance with this Code, data protection risks and other relevant issues.

Each Group Privacy Officer shall provide information relevant to the report to the Corporate Privacy Officer.

Mitigation

16.3 SHV shall, if so indicated, ensure that adequate steps are taken to address breaches of this Code identified during the monitoring or auditing of compliance pursuant to this Article 16.

Audit by Supervisory Authority

16.4 The Lead SA may request an audit of the facilities used by SHV for the Processing of Employee Data for compliance with this Code. In addition, the Supervisory Authority of the EEA country at the origin of Transfer will be authorized to audit the relevant Transfer (including, for the avoidance of doubt, the Data Importer) for compliance with this Code.

Article 17 – Complaints Procedure

Complaints Procedure

17.1 Employees may file a complaint in respect of any claim they have under Article 18.4 or violations of their rights under EEA Data Protection Law:

(i) in accordance with the applicable complaints procedure set forth in the SHV Policies & Guidelines; or

(ii) with the SHV Privacy Function.

Employees may also file a complaint or claim with the Supervisory Authority or competent court in accordance with Article 18.5. The SHV Privacy Function shall be responsible for complaint handling. Each complaint will be assigned to an appropriate Staff member (either within the Privacy Function or within the applicable Business Unit or staff function). The relevant Staff member shall:

(i) promptly acknowledge receipt of the complaint;

(ii) analyse the complaint and, if needed, initiate an investigation; and

(iii) when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

Reply to Employee

17.2 SHV will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Employee within one calendar month of the date that the complaint was filed. SHV shall inform the Employee in writing via the means that the Employee originally used to contact SHV (e.g. via mail or email) either (a) of SHV position with regard to the complaint and any action SHV has taken or will take in response or (b) when he or she will be informed of SHV's position, which date will be no later than two calendar months after the original one month period. The appropriate Staff member shall send a copy of the complaint and his or her written reply to the relevant Group Privacy Officer.

Complaint to Group Privacy Officer

17.3 An Employee may file a complaint with the Group Privacy Officer:

(i) if the resolution of the complaint by the Staff member is unsatisfactory to the Employee (e.g., the complaint is rejected);

(ii) if the Employee has not received a response as required by Article 17.2;

(iii) if the time period provided to the Employee pursuant to Article 17.2 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response; or

(iv) in one of the events listed in Article 7.7.

The procedure described in Articles 17.1 through 17.2 will apply to complaints filed with the Group Privacy Officer. If the handling of the complaint by the Group Privacy Officer is not satisfactory to the Employee, the Employee can file a complaint or claim with the Supervisory Authority or competent court in accordance with Article 18.5.

Where the relevant Group Privacy Officer was involved in the handling of the initial complaint under Article 17.1, the complaint under Article 17.3 will be handled by the Corporate Privacy Officer.

Article 18 – Legal Issues

Interaction with local law

18.1 Employees may enforce the commitments made by SHV under this Code in accordance with this Article 18. These rights are in addition to, and will not prejudice, any other rights or remedies that these Employees may otherwise have against SHV under applicable law.

Law applicable to Code

18.2 This Code will be governed by and interpreted in accordance with Dutch law.

Complaints procedure	18.3	Employees are encouraged (but are not required) to first file a complaint with SHV in accordance with Article 17 before filing a complaint or claim with an SA or court in accordance with Article 18.5.
Third Party Beneficiary Rights	18.4	If SHV violates this Code with respect to its Processing of an Employee's Employee Data, such Employee can as a third party beneficiary enforce any claim as a result of a breach of the articles 2 – 8, 10, 11, 16.4, 17, 18, and 20.
Jurisdiction for Claims of Employees	18.5	In case of a violation of this Code, the affected Employee may, at his or her choice, submit a complaint or a claim (as applicable) under Article 18.4 against SHV Holdings with: (i) the Lead SA or courts in the Netherlands; (ii) the SA in the EEA country where the (a) Employee has his or her habitual residence or place of work, or (b) the infringement took place; (iii) the courts in the EEA country (a) where the Employee has his or her habitual residence, or (b) where the Group Company being the Controller of the relevant Employee Data is established. SHV Holdings accepts liability for a breach by a Group Company or a Third Party Processor located outside the EEA, although SHV Holdings may assert any defense that the relevant non-EEA Group Company or Third Party Processor could have asserted.
Rights of Employees to claim damages and Burden of Proof	18.6	In case an Employee has a claim under Article 18.4, such Employee shall be entitled to compensation of material and non-material damages suffered by such Employee resulting from a violation of this Code to the extent provided by applicable law of the relevant EEA country. To bring a claim for damages, the Employee must demonstrate that he or she has suffered damages and establish facts which show it is likely that the damage has occurred because of a violation of this Code. If SHV Holdings can prove that the Group Company or Third Party Processor located outside the EEA is not responsible for the event giving rise to the damage, it may discharge itself from liability.
Mutual assistance and redress	18.7	All Group Companies will co-operate with and assist each other to the extent reasonably possible to handle: (i) a request, complaint or claim made by an Employee; or (ii) a lawful investigation or inquiry by a competent SA or government authority. The Group Company that receives a request, complaint or claim from an Employee is responsible for handling any communication with the Employee regarding his or her request, complaint or claim except where circumstances dictate otherwise. The Group Company that is responsible for the Processing to which the request, complaint or claim relates, will bear all costs involved and reimburse SHV Holdings.

Cooperation with Competent SA	18.8	SHV shall cooperate with the Competent SA in respect of any inquiry or investigation with regard to this Code and comply with binding decisions or orders of the Competent SA issued on the interpretation and application of this Code.
Mitigation	18.9	SHV Holdings shall ensure that the necessary actions are taken to remedy violations of this Code by a Group Company.

Article 19 – Sanctions for Non-compliance

Non-compliance	19.1	Non-compliance of Employees with this Code may result in appropriate measures in accordance with applicable law up to and including termination of employment.

Article 20 – Conflicts Between this Code and Applicable Local Law

Conflict between Code and law	20.1	Each Group Company shall monitor its local laws and practices and, if it becomes aware that it is or has become subject to laws or practices (including Disclosure Requests) that prevent it from complying with this Code or that have a substantial effect on the protection offered by this Code (including on any Data Protection Impact Assessments or Transfer Impact Assessments performed thereunder), the relevant Group Company will promptly notify SHV Holdings and determine – in consultation with the General Counsel of SHV Holdings and the Group Privacy Officer - how to comply with this Code and address the conflict, including by implementing appropriate supplementary measures in accordance with Article 14.4. The Group Privacy Officer may seek the advice of the Lead SA or another competent public authority.
New conflicting legal requirements	20.2	The relevant Responsible Executive shall promptly inform the Group Privacy Officer if any new legal requirement interferes with SHV's ability to comply with this Code.
Requests for Disclosure of Employee Data	20.3	Subject to the following paragraph, SHV shall inform the Lead SA and – where relevant – the Data Exporter, if SHV becomes aware that applicable local law or practices of a Third Country is likely to have substantial adverse effect on the protection offered by this Code, including if SHV receives a Disclosure Request. Notifications of a Disclosure Request shall include information about the Employee Data requested, the requesting body and the legal basis for disclosure and the provided response. SHV will assess the legality of a Disclosure Request, in particular whether it remains within the powers granted to the requesting authority. SHV will challenge Disclosure Requests that it considers unlawful under the laws of the Third Country, applicable obligations under international law, or principles of international comity, and under the same conditions shall pursue possibilities to appeal. When challenging a Disclosure Request, SHV shall seek interim

measures with a view to suspending the effects of the Disclosure Request until the requesting authority has decided on its merits. SHV shall not disclose the Employee Data requested until required to do so under the applicable procedural rules and will only provide the Employee Data that are strictly necessary when complying with a Disclosure Request, based on a reasonable interpretation thereof. SHV will document this assessment and provide it to the Data Exporter and, upon request, to any Competent SA.

If notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, SHV will inform the Data Exporter to the maximum extent permitted by applicable law, and will use its best efforts to request the relevant authority to waive this prohibition, will document these efforts, and demonstrate them upon request to the Data Exporter. SHV will at regular intervals provide the Data Exporter with as much relevant information as possible on the requests received. This information will be preserved and provided to any Competent SA upon request. In any event, SHV will on an annual basis, or upon request, provide to the Lead SA general information on the number and type of Disclosure Requests it received in the preceding 12-month period, to the fullest extent permitted by applicable law.

In any event, any transfers by SHV of Employee Data in response to a Disclosure Request will not be massive, disproportionate, or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

This Article does not apply to requests received by SHV from other government agencies in the normal course of its activities, which SHV can continue to provide in accordance with applicable law, as far as the request is necessary and proportionate in a democratic society to protect one of the objectives listed in article 23(1) of the GDPR.

Article 21 – Changes to this Code

Approval for Changes	21.1	Any changes to this Code will require the prior approval of the Executive Board of Directors of SHV Holdings and shall thereafter be communicated to the Group Companies. The Corporate Privacy Officer keeps track of and records updates to this Code and will notify any changes including any updates to the list of Group Companies, to the Lead SA on a yearly basis, including a brief explanation of the reasons justifying the update. Where a change affects the protection offered by this Code or significantly affects the Code itself (e.g., changes to the binding character), the Corporate Privacy Officer will promptly communicate these to the Lead SA.
Effective Date of Changes	21.2	Any change will enter into force with immediate effect after it has been approved in accordance with Article 21.1 and is published on the SHV Holdings global intranet and the Group global intranet (as applicable).
Prior Versions	21.3	Any request, complaint or claim of an Employee involving this Code will be evaluated against the version of this Code that is in force at the time the

request, complaint or claim is made.

Article 22 – Transition Periods

Transition period for new Group Companies	22.1	Any entity that becomes a Group Company after the Effective Date shall comply with this Code within two years of becoming a Group Company. During this transition period, no Employee Data will be Transferred until (a) the relevant Group Company has achieved compliance with the Code or (b) an alternative data transfer mechanism has been implemented, such as standard contractual clauses.
Transition period for Divested Entities	22.2	A Divested Entity may remain covered by this Code after its divestment for such period as may be required by SHV to disentangle the Processing of Employee Data relating to such Divested Entity.

Contact details:

SHV Holdings:
privacy@shv.nl

SHV Energy:
dpo@shvenergy.com

Makro (South America):
dataprivacy@makro.com

Mammoet:
privacy@mammoet.com

ERIKS:
privacyoffice@eriks.com

Nutreco:
privacy@nutreco.com

NPM Capital:
privacy@npm-capital.com

http://www.shv.nl/english

ANNEX 1 – Definitions

Adequacy Decision	ADEQUACY DECISION means a decision issued by the European Commission under Article 45(3) of the GDPR that a country or region outside the EEA or a category of recipients in such country or region is deemed to provide an “adequate” level of data protection
Article	ARTICLE means an article in this Code.
Business Purpose	BUSINESS PURPOSE means a purpose for Processing Employee Data as specified in Article 2 or 3 or for Processing Special Categories of Data as specified in Article 4 or 3.
Business Unit Privacy Officer	BUSINESS UNIT PRIVACY OFFICER means the officer as referred to in Article 13.4.
Corporate Privacy Officer	CORPORATE PRIVACY OFFICER means the officer as referred to in Article 13.2.
Code	CODE means this Privacy Code for Employee Data.
Competent SA	COMPETENT SA means any Supervisory Authority competent to audit under Article 16.4.
Controller	CONTROLLER means the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Employee Data.
Data Exporter	DATA EXPORTER means the Group Company that Transfers Employee Data under this Code.
Data Importer	DATA IMPORTER means the Group Company that is the recipient of a Transfer of Employee Data under this Code.
Data Protection Impact Assessment (DPIA)	DATA PROTECTION IMPACT ASSESSMENT (DPIA) means a review procedure to carry out and document an assessment of the impact of an envisaged IT-system or Processing on the protection of Employee Data and Employee privacy rights. The DPIA will be performed prior to implementation of the envisaged IT-system or Processing and will regard the entire lifecycle management of Employee Data, from collection to processing to deletion. A DPIA contains a description of: • the relevant SHV Group Companies and third parties responsible for the Processing; • the envisaged Processing; • the Processing Purpose for which Employee Data is Processed; • security measures; • data retention periods; and • categories of recipients; • any transfers of Employee Data to a Third Country, including

suitable transfer mechanisms;

and an assessment of:

- the necessity and proportionality of the envisaged Processings;
- the risks to the privacy rights of Employees including a description of mitigating (privacy-by-design and privacy-by-default) measures to minimize these risks; and
- the context of the Processing.

Data Security Breach

DATA SECURITY BREACH means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Employee Data transmitted, stored or otherwise Processed. A Data Security Breach will be deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Data by an Employee of SHV or Third Party Processor or an individual acting under their respective authority, if:

(i) the acquisition, access, or use of Data was made in good faith and within the course and scope of the employment or professional relationship of such Employee or other individual; and

(ii) the Data is not further acquired, accessed, used or disclosed by any person.

Dependant

DEPENDANT means the spouse, partner or child belonging to the household of the Employee or emergency contact of the Employee.

Divested Entity

DIVESTED ENTITY means the divestment by SHV or a Group of a Group Company or business by means of:

(i) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company; and/or

(ii) a demerger, sale of assets, or any other manner or form.

Disclosure Request

DISCLOSURE REQUEST means a legally binding request for disclosure of (or direct access to) Employee Data from a law enforcement authority or state security body of a Third Country.

EEA

EEA or EUROPEAN ECONOMIC AREA means all member states of the European Union, plus Norway, Iceland and Liechtenstein, and for purposes of this Code, Switzerland. SHV's General Counsel can decide to include other countries in this definition, provided that such country is subject to an Adequacy Decision.

EEA Data Protection Law

EEA Data Protection Law means the GDPR as well as provisions of mandatory law of an EEA country containing rules for the protection of individuals with regard to the Processing of Employee Data including security requirements for and the free movement of such Employee Data.

Effective Date

EFFECTIVE DATE means the date on which this Code becomes effective as set forth in Article 1.6.

Employee	EMPLOYEE means the following identified or identifiable persons: (i) an employee, job applicant or former employee of SHV, including temporary workers working under the direct supervision of SHV (e.g. independent contractors and trainees). This term does not include people working at SHV as consultants or employees of Third Parties providing services to SHV; and (ii) a (former) executive or non-executive director of SHV or (former) member of the supervisory board or similar body to SHV.
Employee Data or Data	EMPLOYEE DATA or DATA has the meaning given to that term in Article 1.1.
Employment-at-will	EMPLOYMENT-AT-WILL means an employment relationship in which either the employer or employee can terminate the employment relationship at any time for any reason, with or without advance notice.
General Counsel	GENERAL COUNSEL means the general counsel of SHV Holdings.
General Data Protection Regulation or GDPR	GENERAL DATA PROTECTION REGULATION or GDPR means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data or any successor or replacement thereof.
Group	GROUP means a collection of Group Companies or legal entities active in a certain field, in any case SHV Holdings, ERIKS, Makro, Mammoet, NPM Capital, SHV Energy and Nutreco.
Group Company	GROUP COMPANY means SHV Holdings and any company or legal entity in respect of which SHV Holdings, directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such company or legal entity; however, any such company or legal entity shall be deemed a Group Company only as long as: (i) a liaison and/or relationship exists with SHV Holdings; (ii) it is covered by the SHV Policies & Guidelines; and (iii) SHV Holdings, directly or indirectly, is able to require such Group Company to abide by this Code. For the avoidance of doubt, a participation held by NPM Capital N.V. (whether a minority or majority participation) shall not qualify as a Group Company in and for the purposes of this Code, as a result of which this Code shall not apply to any participations of NPM Capital N.V.
Group Ethics and Compliance Committee	GROUP ETHICS AND COMPLIANCE COMMITTEE means the committee established within a Group referred to in Article 13.5.
Group Privacy Officer	GROUP PRIVACY OFFICER means a privacy officer within a Group

	appointed pursuant to Article 13.4.
Lead SA	LEAD SA means the Supervisory Authority of the Netherlands.
Processing	PROCESSING means any operation or set of operations that is performed on Employee Data, whether or not by automated means, such as collection, recording, storage, organisation, structuring, adaptation or alteration, retrieval, consultation, use, disclosure (including the granting of remote access) by transmission, dissemination or otherwise making available, alignment or combination, restriction erasure or destruction of Employee Data.
Processing Purpose	PROCESSING PURPOSE has the meaning given to that term in Article 3.2.
Records of Processing Activities	RECORDS OF PROCESSING ACTIVITIES means a record of Processing activities maintained in writing, including in electronic form, by SHV that contains the following information: a. the name and contact details of the SHV Group Company that is the Controller; b. the Processing Purposes; c. the categories of Employee Data; d. the categories of recipients to whom Employee Data have been disclosed; e. where applicable, information about transfers of Employee Data to a Third Country; f. where possible, the envisaged retention periods; and g. where possible, a general description of the measures under Article 8.1.
Responsible Executive	RESPONSIBLE EXECUTIVE means for SHV Holdings and the Groups, the Employee that is accountable for compliance with the Code, being the chief executive officer of respectively SHV Holdings and the relevant Group.
Supervisory Authority or SA	SUPERVISORY AUTHORITY OR SA means any data protection authority of one of the countries of the EEA.
Secondary Purpose	SECONDARY PURPOSE means any purpose for which Employee Data is further Processed that is other than the purpose for which the Employee Data was originally collected.
Special Categories of Data	SPECIAL CATEGORIES OF DATA means Employee Data that reveal an Employee's racial or ethnic origin, political opinions or membership in political parties or similar organisations, religious or philosophical beliefs, membership in a professional or trade organisation or union, physical or mental health including any opinion thereof, disabilities, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behaviour, social security numbers issued by the government, or genetic and biometric data for the purpose of uniquely identifying a natural person.

SHV	SHV means SHV Holdings and all its Group Companies.
SHV Holdings	SHV HOLDINGS means SHV Holdings N.V., having its registered office at Rijnkade 1, 3511LC, Utrecht, the Netherlands, registered with the chamber of commerce under number 30065974, which can be contacted via info@shv.nl of privacy@shv.nl.
SHV Holdings Ethics and Compliance Committee	SHV HOLDINGS ETHICS AND COMPLIANCE COMMITTEE means the committee established within a Group and SHV Holdings referred to in Article 13.3.
SHV Privacy Function	SHV PRIVACY FUNCTION means the function as referred to in Article 13.1.
Staff	STAFF means all Employees and other persons acting under the direct authority of SHV who Process Employee Data as part of their respective duties or responsibilities towards SHV using SHV information technology systems or working primarily from SHV's premises.
Third Country	THIRD COUNTRY means a country outside the EEA to which Employee Data is transferred, where such transfer is not covered by an Adequacy Decision.
Transfer	TRANSFER means a transfer (or set of transfers), including disclosure of, or remote access to, Employee Data under this Code to a Group Company in a Third Country.
Transfer Impact Assessment	TRANSFER IMPACT ASSESSMENT means an assessment on whether, taking into account the specific circumstances of the Transfer, the laws and practices of the Third Country, including those requiring the disclosure of Employee Data to public authorities or authorizing access by such authorities, prevent SHV from fulfilling its obligations under this Code. In assessing the laws and practices of the Third Country, SHV shall take into account in particular: a. the specific circumstances of the Transfers, and any envisaged onward Transfers within the same Third Country or to another Third Country, including: i. purposes for which the data are Transferred and Processed (e.g. marketing, HR, storage, IT support, clinical trials); ii. types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfers); iii. sector in which the Transfers occur; iv. categories and format of the Employee Data Transferred; v. location of the Processing including storage; vi. transmission channels used. b. the laws and practices of the Third Country relevant in light of

the circumstances of the Transfers, including requirements to disclose Employee Data to public authorities or authorizing access by such authorities as well as the applicable limitations and safeguards. This also includes laws and practices providing for access to Employee Data during transit between the country of the Data Exporter and the Third Country;

c. any relevant contractual, technical or organizational safeguards put into place to supplement the safeguards under this Code, including measures applied during transmission and to the Processing of Employee Data in the Third Country.

Third Party	THIRD PARTY means any person, private organisation or government body outside SHV.
Third Party Controller	THIRD PARTY CONTROLLER means a Third Party that Processes Employee Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR means a Third Party that Processes Employee Data on behalf of SHV that is not under the direct authority of SHV.

Interpretations

INTERPRETATION OF THIS CODE:

(i) unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time;

(ii) headings are included for convenience only and are not to be used in construing any provision of this Code;

(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(iv) if not already indicated, the male form shall include the female form;

(v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa;

(vi) a reference to a document (including, without limitation, a reference to this Code) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Code or that other document; and

(vii) a reference to law includes any regulatory requirement, sectorial recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.

ANNEX 2 – Description of Processing of Employee Data

1. Categories of Employee Data

Category of Employee Data	Examples of Employee Data Elements
Basic personal details	Name, employee identification number, work contact details (email, phone numbers, physical address)
Other personal Details	Home contact details (email, phone numbers, physical address), language(s) spoken, gender, date of birth, national identification number, social security number, marital/civil partnership status, domestic partners, dependents, emergency contact information
Documentation required under immigration laws	Citizenship, passport data, details of residency or work permit
Compensation and payroll	Base salary, bonus, benefits, compensation type, salary step within assigned grade, details on stock appreciation rights and other awards, currency, pay frequency, effective date of current compensation, salary reviews, banking details, working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date
Position information	Description of current position, job title, corporate status, management category, job code, salary plan, pay grade or level, job function(s) and subfunction(s), company name and code (legal employer entity), branch/unit/department, location, employment status and type, full-time/part-time, terms of employment, employment contract, work history, hire/re-hire and termination date(s) and reason, length of service, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information
Talent management information	Details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates), details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate, driver's license information, and information used to populate employee biographies
Management records	Details on directorships and appointments, board minutes, board decisions
System and application access data	Information required to access company systems and applications such as user and system IDs for company network or servers, email account, instant messaging account, passwords, access logs, activity logs, and electronic content produced by Data Subjects using company systems
Racial or ethnic data	Photos (e.g. a copy of a passport containing a photo) and video images which, in some countries, qualify as racial or ethnic data
Physical or mental health data	Any information or opinion of physical or mental health and data relating to disabilities, disability status, and absence due to illness or pregnancy
Criminal data	Information relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior.

Sexual preference	Information on sexual preference
Biometric data	Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person

2. Purposes for which Employee Data is Processed

Category of Group Companies	Purpose of Processing	Examples of Processing Activities
All Group Companies	Managing Workforce	Managing work activities and personnel generally, including recruitment, appraisals, performance management, promotions and succession planning, rehiring, administering salary, and payment administration and reviews, wages and other awards such as stock appreciation rights and bonuses, healthcare, pensions and savings plans, training, leave, managing sickness leave, promotions, transfers, secondments, honoring other contractual benefits, providing employment references, loans, performing workforce analysis and planning, performing employee surveys, performing background checks, managing disciplinary matters, grievances and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, workforce reporting and data analytics/ trend analysis, and creating and maintaining one or more internal employee directories.
All Group Companies	Workforce Analytics	Analytics for succession planning, workforce management, and data security, such as, analytics to assist in planning succession and to ensure business continuity, to design employee retention programs and diversity initiatives, to offer training opportunities and to identify patterns in the use of technology systems to information entrusted to SHV as well as to protect SHV's people and property.
All Group Companies	Communications, Facilities and Emergencies	Facilitating communication with employees, ensuring business continuity and crisis management, providing references, protecting the health and safety of employees and others, safeguarding and maintaining IT infrastructure, office equipment, facilities and other property, facilitating communication with employees and

		their nominated contacts in an emergency.
All Group Companies	Business Operations	Operating and managing the IT, communications systems and facilities, managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, re-organizations or disposals and integration with upon mergers or acquisitions.
All Group Companies	Monitoring	Monitoring compliance with the SHV Codes of Conduct or other SHV policies and internal policies, including pursuant to SHV's policies and procedures with regard to monitoring of telephone, email, Internet and other company resources, and other monitoring activities as permitted by applicable law.
All Group Companies	Compliance	Complying with legal and other requirements, such as income tax and national insurance deductions, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation, and managing any internal complaints or claims (including those received through the Speak Up Line), conducting investigations including employee reporting of allegations of wrongdoing, policy violations, fraud, or financial reporting concerns, and complying with internal policies and procedures.

3. Purposes for which Special Categories of Data are are Processed

Category of Group Companies	Purpose of Processing	Examples of Processing Activities
All Group Companies	Security and facility access	In some countries photos and video images of Employees qualify as Special Categories of Data. SHV may process photos (e.g. a copy of a passport containing a photo) and video images for the protection of (the interests and assets of) SHV, its Employees, joint ventures, participations, customers, suppliers and business partners

Category of Group Companies	Purpose of Processing	Examples of Processing Activities
		(including safeguarding the integrity of SHV, pre- and in- employment screening of Employees and monitoring of Employees), to record decisions made in the course of business for future reference (e.g. when Employees participate in video conferencing which is recorded), for site access and security reasons, demographic reporting under applicable anti-discrimination laws, for obtaining visa's, permits and technology export licenses and for inclusion in Employee directories.
All Group Companies	Preferential status based on ethnicity or culture	Providing preferential status to persons from particular ethnic or cultural minorities to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Special Categories of Data allows for an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection against the relevant Processing.
All Group Companies	Health services	Providing health services to an Employee provided that the relevant health data is processed by or under the supervision of a health professional who is subject to professional confidentiality requirements.
All Group Companies	Administering pensions and benefits	Administering pensions, health and welfare benefit plans, maternity, paternity or family leave programmes, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee.
All Group Companies	Preferential status based on health status	Providing preferential status to persons with a particular disability to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Special Categories of Data allows for an objective determination that an Employee belongs to the relevant category and the Employee has not filed a written objection against the relevant Processing
All Group Companies	Re-integration and support	Reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity.
All Group Companies	Pre- and in-employment screening	Pre- and in-employment screening and monitoring of Employees and for assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities.
All Group Companies	Facility management	Providing facilities in the workplace to accommodate health problems or disabilities.
All Group Companies	Background checks	Assessing an application by an Employee to make

Category of Group Companies	Purpose of Processing	Examples of Processing Activities
		a decision about the Employee or provide a service to the Employee
All Group Companies	Screening for criminal activities	Protecting the interests of SHV, its Employees, joint ventures, participations, customers, suppliers and business partners with respect to criminal offences that have been or, given the relevant circumstances are suspected to be or have been, committed against SHV, its Employees, joint ventures, participations, customers, suppliers and business partners, and further for pre- and in-employment screening and monitoring of Employees.
All Group Companies	Administering employee pensions, benefits, and memberships	Processing data on sexual preference (including data relating to partners of Employees) for the purpose of administering Employee pensions, benefits programs, and memberships.
All Group Companies	Accommodating religious or philosophical practices	Processing data on religious or philosophical beliefs insofar as necessary for accommodating religious or philosophical practices, dietary requirements or religious holidays.
All Group Companies	Biometric security	Biometric security and access management purposes in relation to SHV's premises and systems.