INTERNAL DATA PROTECTION POLICY

PURPOSE AND SCOPE OF THIS POLICY

Asco Industries NV (**"the Company"**, "**we**" or "**us**") handles large amounts of information as part of its business activities.

Some of that information relates to individuals and therefore qualifies as Personal Data. The large majority of the Personal Data that we handle relates to:

- *our employees,*
- *contractors,*
- *temporary workers,*
- *students and trainees,*
- *job applicants,*
- *individuals employed or engaged by our customers, partners and suppliers*

("**Data Subjects**").

You can find examples of categories of Personal Data in SCHEDULE 1.

This Policy will apply to any operation that is performed on Personal Data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, combination, restriction, erasure or destruction ("**Processing**").

Personal Data are vulnerable by their nature and any inappropriate use or unauthorized loss, modification or disclosure of these data may have a significant negative impact on the relevant Data Subjects. Therefore, Personal Data are subject to strict data protection laws and regulations. These laws and regulations restrict the manner in which we can use Personal Data. Violations of these laws and regulations

may result in sanctions being imposed upon the Company and/or the Company being held liable to pay damages.

This internal Data Protection Policy ("**Policy**") is not intended to prevent the use of Personal Data. Instead, the purpose of this Policy is to provide a uniform framework for the protection of Personal Data relating to the Data Subjects in accordance with the needs of the Company and the Data Subjects' legal rights as set out in applicable laws and regulations.

For operational direction and support, please refer to supporting guidance by the Data Protection Director and the Legal Department.

DUTY TO COMPLY WITH POLICY

All Company employees and independent contractors are required to comply with this Policy. Heads of Company departments and Company subsidiaries must take appropriate and reasonable steps to make the terms of this Policy binding on their directors, officers, employees, contract labor, agents and other representatives, including disciplinary action for violations.

The Company recognizes that laws and regulations may require stricter standards than those set out in this Policy. If and to the extent that laws and regulations impose data protection requirements that are stricter than the standards set out in this Policy, the Company must Process Personal Data in accordance with such laws and regulations. Where applicable laws and regulations provide a level of data protection that is lower than the standards set out in this Policy, the Company will Process Personal Data in accordance with such laws and regulations.

KEY DATA PROTECTION PRINCIPLES

Anyone who Processes Personal Data, must do so in accordance with the following principles.

Personal Data must be:

- Processed based on a legal ground (**conditions for Processing**)
- Processed for limited purposes (**purpose limitation principle**)
- Processed in a transparent manner vis-à-vis the Data Subject (**transparency principle**)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed (**data minimization principle**)
- Accurate and, where necessary, kept up to date (**accuracy principle**)
- Kept no longer than necessary in relation to the purposes for which they are Processed and then destroyed or anonymized (**retention limitation principle**)
- Processed in line with Data Subjects' rights
- Handled securely and confidentially (**integrity and confidentiality principle**)
- Only transferred to Company subsidiaries or third parties if permitted or required by law and subject to additional safeguards that may be appropriate or required by applicable law

1 Conditions for Processing

Anyone who Processes Personal Data, may do so only if one (or more) of the following conditions have been fulfilled:

- The Data Subject has consented to the Processing. The consent must be freely given, specific, informed and unambiguous;
- The Processing is necessary:
    - in relation to a contract which the Data Subject has entered into (e.g. Processing contact details of the contact person within a third party we entered into an agreement with or Processing an employee's salary information and bank account details so that the Company can pay his/her salary); or

- because the Data Subject has asked the Company for something to be done so he/she can enter into a contract;

– The Processing is necessary because of a legal obligation that applies to the Company (other than obligations resulting from a contract) (e.g. reporting salary data of employees to social security or tax authorities);
– The Processing is necessary to protect the Data Subject's "vital interests". This condition only applies in cases of life or death (e.g. where a Data Subject's medical history is disclosed to a hospital treating him/her after a life-threatening accident at work); and
– The Processing is necessary for the legitimate interests of the Company (or of any third party to whom the Personal Data are disclosed) and those interests are not overridden by the interests or fundamental rights of the Data Subjects whose Personal Data are being Processed (e.g. Processing of certain employee Personal Data for physical security, IT/network security).

Stricter conditions apply when Processing certain categories of Personal Data which are considered to be sensitive[1]. In most cases we can only Process sensitive Personal data if:

– The Data Subject has given consent to the Processing; or
– The Processing is necessary to comply with a legal obligation.

Being able to satisfy a condition for Processing will not on its own guarantee that the Processing complies with this Policy and applicable privacy laws and regulations. The other data protection principles set out in this Policy must also be complied with.

2 Purpose limited Processing (purpose limitation principle)

[1] For example: data concerning physical and mental health, conditions or treatments; disability data; medical records; data revealing racial or ethnic origin, political adherence or opinions, religious or philosophical beliefs, trade union membership; Genetic data; biometric data for the purpose of uniquely identifying a Data Subject; Data concerning a Data Subject's sex life or sexual orientation; Data relating to criminal or administrative convictions and offences or related security measures.

Personal Data may only be collected and Processed for specified and lawful purposes and Personal Data may not be Processed in a manner incompatible with those purposes, except if this is:

- Expressly required or authorized by law;
- Necessary to comply with a legal obligation.

3 Transparent Processing (transparency principle)

Unless this would involve a disproportionate effort or if the Data Subject is already aware of this, the Company must ensure that Data Subjects understand:

- **Who** the Controller is (usually the Company or Company subsidiaries that Process the Personal Data);
- **Why** we Process their Personal Data;
- **How** their Personal Data will be Processed;
- **To whom the data may be disclosed** (such as clients and/or Company subsidiaries);
- **Where** their Personal Data will be **transferred** to or be accessible from;
- **What** their **rights** are in relation to their Personal Data under applicable law;
- **How long** their Personal Data will be retained;
- The **legal ground(s)** on the basis of which we Process their Personal Data (see the section about conditions for Processing in this Policy); and
- Such other aspects as may be required by the circumstances (e.g. explain the legitimate interest for which the Company Processes Personal Data).

4 Adequate, relevant and limited to what is necessary in relation to the purposes (data minimization principle)

Personal Data should only be Processed to the extent that it is adequate and relevant to achieve our purposes. Any Personal Data which is not necessary for our purposes should not be collected in the first place.

Also, reasonable steps must be taken to retain the Personal Data only for as long as is necessary to achieve our purposes.

5 Accurate and, where necessary, kept up to date (accuracy principle)

We must ensure that the Personal Data that we hold is kept accurate and up to date.

Personal Data which is incorrect or misleading is not accurate and, therefore, steps should be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

6 Kept no longer than necessary in relation to the purposes for which they are Processed and then destroyed or anonymized (retention limitation principle)

Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed.

Any Personal Data must be retained and disposed of in accordance with the Company Data Retention Policy. When litigation is threatened or occurs, information relevant to the dispute must be kept, even if it is no longer needed for its original purpose, until it is no longer needed for threatened, actual, or reasonably foreseeable litigation.

7 Processed in line with the Data Subjects' rights

Data Subjects have the following rights in respect of the Personal Data that we hold about them:

- Right to be informed about the Processing of their Personal Data;
- Right to access to their Personal Data;
- Right to rectification of their Personal Data;
- Right to erasure of their Personal Data;
- Right to restriction of the Processing;
- Right to portability of their Personal Data;
- Right to withdraw their consent to the Processing of their Personal Data;
- Right to object to the Processing;
- Right to not be subject to automated decisions, including profiling; and
- Right to lodge a complaint about the Processing of their Personal Data.

The Company maintains procedures to allow Data Subjects to exercise any of the above rights vis-à-vis the Company.

Also, you should not make important decisions about an individual based exclusively on fully automated Processing without:

- Obtaining the prior approval from Data Protection Director and the Legal Department; and
- Explaining automated Processing and its underlying logic to the Data Subject; and
- Providing a mechanism for the appeal or review of such decisions by a human decision maker.

8 Handled securely and confidentially (integrity and confidentiality principle)

The Company will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of each Processing activity (including, in particular, the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed).

When determining such measures we must take into account various factors including the following:

- Security best practices;
- The costs of implementation of such measures;
- The nature, scope, context and purposes of the Processing; and
- The potential impact on and risks for the Data Subjects.

Any Personal Data Breaches must be handled in accordance with the Personal Data Breach Handling Policy.

9 Transfer of Personal Data

General – The Company may share Personal Data internally (e.g. Personal Data is shared between one or more Company subsidiaries) or externally with third parties (e.g. Personal Data is shared with an external vendor) only if the Personal Data is shared:

- in accordance with this Policy; and
- for any of the purposes for which the Company collects the Personal Data.

The recipient to whom Personal Data are transferred will either be a Controller or a Processor. Also, the transfer may be across national borders.

Transfers within the Company – For the efficient operation of our business and the effective management of our human resource functions, the Company may share Personal Data between various subsidiaries or between various organizational components.

Transfers outside the Company – The Company may have to transfer Personal Data to recipients outside the Company.

The Company may transfer Personal Data to *external vendors* so that the latter can provide services or products to the Company (eg. a payroll service provider (*sociaal secretariat / Secrétariat social*)). Many of these vendors will be Processors. The Company will only transfer Personal Data to reliable vendors that have been carefully selected by the Company and that have concluded a contract that contains data

protection provisions that have been approved by the Chief Human Resources Officer. Where Personal Data is transferred to a vendor that is a Controller, the Company will only transfer Personal Data to such vendor if there is a sufficient legal basis for doing so (e.g. if the Company is required by law to share the data with a third party; if the Data Subject has given his/her prior consent; etc.).

The Company may transfer Personal Data to *other third* parties (e.g. sharing employee salary data to social security or tax authorities; e.g. sharing a Data Subject's medical history to a hospital treating him/her after a life-threatening accident at work; etc.). The Company will only transfer Personal Data to such third parties if there is a sufficient legal basis for doing so (e.g., when the Company is required by law to share the data with a third party).

Transfers across borders – We may only transfer Personal Data to recipients in countries outside the European Economic Area (**EEA**)[2], if such non-EEA country is white-listed by the EU as providing a level of data protection that is equivalent to the level of data protection afforded by the EU. The EU has so far recognised Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, Uruguay, the UK, and the US (limited to the "EU-US Data Privacy Framework") as providing adequate protection. You can find more information about the white-listed countries on the EU Commission's website.

Note that the term transfer should be interpreted broadly and includes any instance where we send Personal Data to third parties, give them access to Personal Data (even remotely), have Personal Data hosted by them, etc. Examples of transfers include:

- An Indian IT supplier accesses our CRM database (which is based in Belgium and which contains Personal Data) in order to provide application maintenance and support services
- We use a cloud application based in the US to handle Personal Data relating to our employees

2 The European Economic Area consists of all the member states of the European Union plus Iceland, Liechtenstein and Norway.

You should not allow any Personal Data to be transferred to recipients based in a non-EEA country that is not white-listed, without:

- Obtaining the prior approval from Data Protection Director and the Legal Department; and
- Having put in place certain adequacy safeguards (eg. concluding EU approved contract clauses with the recipient).

ACCOUNTABILITY

Our goal is to be a privacy-accountable organisation. That means that it is our responsibility not only to comply with this Policy and with any applicable data privacy laws and regulations, but also to demonstrate on an ongoing basis that we comply.

Therefore, we have implemented and we will maintain the following measures:

- **Data Protection Director –** We have appointed a Data Protection Director whose primary responsibility is to foster a culture of data protection compliance across all the Company's business units and Company subsidiaries.

- **Records of Processing activities –** The Data Protection Director maintains a central inventory of all our Processing activities.

- **Audit of Compliance –** The Company's organizational components that Process Personal Data, must submit their Processing practices to an audit to verify compliance with this Policy and applicable privacy laws and regulations. Audits of compliance with this Policy shall be conducted on a regular basis.

  If any audit reveals any failure to comply with this Policy or with any applicable data privacy laws and regulations, the Company will take action to remediate such gap and to avoid any re-occurrence of such gap.

- **Training and Supervision –** Employees with access to Personal Data will be given appropriate training in the proper way to handle such Personal Data as well as how to respond to inquiries from Data Subjects about the Processing of their Personal Data.

  [Employees with access to Personal Data will be required to agree to handle Personal Data in accordance with this Policy, will be subject to appropriate supervision].

- **Privacy by Design, Privacy by Default, Privacy Impact Assessments –** We implement measures that meet the principles of data protection by design[3] and data protection by default[4]. Where appropriate, we will conduct data protection impact assessments before deciding to Process Personal Data.

COOPERATION WITH DATA PROTECTION AUTHORITIES

When we are requested to cooperate with Data Protection Authorities having jurisdiction over the Personal Data that we Process, we will do so. This may include providing them with access to our premises, employees and systems; responding timely and adequately to their requests; etc.

The Data Protection Director and the Legal Department must be involved in any interaction with any Data Protection Authority.

THE COMPANY ACTING AS PROCESSOR

[3] Privacy by design means that, at every stage of the development of a system or process that will use Personal Data (and during the entire lifecycle of the data Processing), we must build in appropriate privacy safeguards (such as pseudonymisation and data minimisation).

[4] Privacy by default means that, when a system provides the user with a choice with respect to the processing of his or her Personal Data and the individual does not take any action to express a preference, by default the system will process the Personal Data in the least privacy-invasive manner. This obligation applies to the amount of Personal Data collected via the system, the extent of their Processing, the period of their storage and their accessibility.

Although this does not occur often, we may be Processing Personal Data as a Processor on behalf of a Controller (e.g. when we Process Personal Data merely for and on behalf of a customer). In that case, we:

- Commit to Process the Personal Data only on instructions from the Controller; and
- Will enter into a written agreement with the Controller that contains appropriate data protection provisions.

NEED MORE INFORMATION?

Questions regarding compliance with this Policy or with privacy laws and regulations may be addressed to the Data Protection Director.

Najib Bardid
Compliance Manager
+32 2 716 07 90
najib.bardid@ascoindustries.com

SCHEDULE 1. DEFINITIONS

"**Controller**" means the legal person that determines the purposes for which and the manner in which Personal Data is Processed. It can do this either on its own or jointly or in common with other organisations. This means that the Controller exercises overall control over the 'why' and the 'how' of a data Processing activity.

"**Data Protection Director**" means the Tax, Risk and Compliance Director whose responsibility is to foster a culture of data protection compliance across all the Company's business units and Company subsidiaries

"**Personal Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by or on behalf of the Company.

"**Processor**" means the entity which Processes Personal Data on behalf of and in accordance with the instructions of the Controller.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.