OREGON TOOL

# Binding Corporate Rules:

# Processor Policy

OREGON TOOL

# Contents

OREGON TOOL

# Part I: Introduction

This Binding Corporate Rules: Processor Policy ("**Processor Policy**") establishes Oregon Tool, Inc. and its affiliates' ("**Oregon Tool**") approach to compliance with Applicable Data Protection Laws (and, in particular, the laws in the EEA) when Processing Personal Information on behalf of a third-party Controller.

## A. Scope of this Processor Policy

This Processor Policy applies when we Process Personal Information as a Processor on behalf of a third-party Controller who is not a Group Member, including when the Personal Information is transferred to a Group Member for Processing outside of the EEA. This Processor Policy applies regardless of whether our Group Members Process Personal Information by manual or automated means.

The standards described in this Processor Policy are worldwide standards that apply to all Group Members when Processing any Personal Information as a Processor. As such, this Processor Policy applies regardless of the origin of the Personal Information that we Process, the country in which we Process Personal Information, or the country in which a Group Member is established.

## B. Types of Personal Information within the scope of this Processor Policy

This Processor Policy applies to all Personal Information that we Process as a Processor on behalf of a third-party Controller (referred to as the "**Customer**" in this Processor Policy), such as processing or fulfilment of Customer orders in the context of providing a service to our Customers. Additional details about the material scope of this Processor Policy are provided in Appendix 10.

### C. Our collective responsibility to comply with this Processor Policy

All Group Members and their staff must comply with this Processor Policy when Processing Personal Information as a Processor on behalf of a Customer, irrespective of the country in which they or the Customer are located.

In particular, all Group Members who Process Personal Information as a Processor must comply with:

- the rules set out in **Part II** of this Processor Policy;
- the practical commitments set out in **Part III** of this Processor Policy;
- the third-party beneficiary rights set out in **Part IV**; and
- the related policies and procedures appended in **Part V** of this Processor Policy. The Appendices form an integral part of the Processor Policy.

### D. Responsibility towards the Customer

As a Processor, Oregon Tool will have a number of direct legal obligations under Applicable Data Protection Laws. In addition, the Customer will also pass certain data protection obligations on to Oregon Tool in its contract appointing Oregon Tool as its Processor. If Oregon Tool fails to comply with the terms of its Processor appointment, this may put the Customer in breach of its Applicable Data Protection Laws and the Customer may initiate proceedings against Oregon Tool for breach of contract, resulting in the payment of compensation or other judicial remedies.

A Customer may enforce this Processor Policy against any Group Member that is in breach of it. Where a non-EEA Group Member (or a non-EEA third-party Processor appointed by a Group Member) Processes Personal Information for which the Customer is a Controller in breach of either (i) this Processor Policy or (ii) the contract with the Customer, that Customer may enforce the Processor Policy against OREGON TOOL EUROPE SA. The Customer may also enforce the Processor Policy against OREGON TOOL EUROPE SA in case of a breach of the written agreement between a Group Member and an external sub-Processor established outside of the EEA. In such event, OREGON TOOL EUROPE SA will be responsible for demonstrating that such Group Member (or third-party Processor) is not responsible for the breach, or that no such breach took place.

When a Customer transfers Personal Information to a Group Member for Processing in accordance with this Processor Policy, a copy of this Processor Policy shall be incorporated into the contract with that Customer. If a Customer chooses not to rely upon this Processor Policy when transferring Personal Information to a Group Member outside the EEA, that Customer is responsible for implementing other appropriate safeguards in accordance with Applicable Data Protection Laws.

### E. Management commitment and consequences of non-compliance

Oregon Tool's management is fully committed to ensuring that all Group Members and their staff comply with this Processor Policy at all times.

Non-compliance may cause Oregon Tool to be subject to sanctions imposed by competent data protection authorities and courts, and may cause harm or distress to individuals whose Personal Information has not been protected in accordance with the standards described in this Processor Policy.

In recognition of the seriousness of these risks, Team Members who do not comply with this Processor Policy will be subject to disciplinary action, up to and including termination.

### F. Relationship with Oregon Tool's Binding Corporate Rules: Controller Policy

This Processor Policy applies only to Personal Information that Oregon Tool Processes as a Processor in order to provide a service to a Customer.

Oregon Tool has a separate Binding Corporate Rules: Controller Policy ("**Controller Policy**") that applies when it Processes Personal Information as a Controller (i.e., for its own purposes). When a Oregon Tool Group Member Processes Personal Information as a Controller, it must comply with the Controller Policy.

In some situations, Group Members may act as both a Controller and a Processor. Where this is the case, they must comply both with this Processor Policy and also the Controller Policy as appropriate. If there is any doubt which policy applies to you, please contact the Group Data Protection Officer ("**Group DPO**") whose contact details are provided below.

### G. Where this Processor Policy is made available

This Processor Policy is accessible on Oregon Tool's corporate website at www.oregontool.com.

### H. Important terms used in this Processor Policy

For the purposes of this Processor Policy:

- the term **Applicable Data Protection Laws** includes the data protection laws in force in the territory from which the Controller of the Personal Information is located. Where a Group Member Processes Personal Information on behalf of an EEA-based Controller under this Processor Policy the term Applicable Data Protection Laws shall include the data protection laws applicable to that Controller in the EEA (including the European Union's General Data Protection Regulation or "GDRP");
- the term **Controller** means the natural or legal person which, alone or jointly with others, determines the purposes and means for the Processing of the Personal Information;

- the term **Customer** refers to the third-party Controller for whom Oregon Tool Processes Personal Information. This includes Oregon Tool's third-party Customers, when we Process Personal Information on their behalf in the course of providing data Processing services to them.
- the term **Data Protection Authority** means the supervisory authority in an EEA Member State;
- the term **EEA** as used in this Policy refers to the Member States of the European Economic Area – that is, the Member States of the European Union plus Norway, Lichtenstein and Iceland;
- the term **Group Member** means the members of Oregon Tool's group of companies listed in Appendix 1;
- the term **Personal Information** means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- the term **Privacy by Design** refers to the principle that a Controller shall implement appropriate technical and organisational measures which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into a Processing activity in order to protect the rights of individuals and meet the requirements of Applicable Data Protection Laws;
- the term **Privacy by Default** refers to the principle that a Controller shall implement appropriate technical and organisational measures to ensure that, by default, only Personal Information which are necessary for each specific Processing purpose are collected, stored, Processed and are accessible; in particular, that by default Personal Information is not made accessible to an indefinite number of people without the individual's intervention;
- the term **Processing** (or **Process)** means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, 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;
- the term **Processor** means a natural or legal person which Processes Personal Information on behalf of a Controller (for example, Oregon Tool is a Processor of the Personal Information it Processes to provide services to its Customers).
- the term **Sensitive Personal Information** means information that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. It also includes information about

an individual's criminal offences or convictions, as well as any other information deemed sensitive under Applicable Data Protection Laws;

- the term **Team Members** refers to all employees, new hires, individual contractors and consultants, and temporary staff engaged by any Oregon Tool Group Member. All Team Members must comply with this Processor Policy.

## I. How to raise questions or concerns

If you have any questions regarding this Processor Policy, your rights under this Processor Policy or Applicable Data Protection Laws, or any other data protection issues, you may contact Oregon Tool's Group DPO (see details below). Oregon Tool's Group DPO will either deal with the matter directly or forward it to the appropriate person or department within Oregon Tool to respond.

| | |
|---|---|
| **Attention:** | Group Data Protection Officer |
| **Email:** | privacy@oregontool.com |
| **Address:** | Oregon Tool Europe SA<br>Rue Emile Francqui, 5<br>1435 Mont-Saint-Guibert<br>Belgium |

| | |
|---|---|
| **Attention:** | Privacy Team |
| **Email:** | privacy@oregontool.com |
| **Address:** | Oregon Tool, Inc.<br>4909 SE International Way,<br>Portland, OR 97222-4679, USA |

Oregon Tool's Group DPO is responsible for ensuring that changes to this Policy are notified to the Group Members and to the individuals whose Personal Information is Processed by Oregon Tool in accordance with Appendix 8.

If you want to exercise any of your data protection rights, please see the Data Protection Rights Procedure set out in Appendix 2. Alternatively, if you are unhappy about the way in which Oregon Tool has used your Personal Information, you can raise a complaint in accordance with our Complaint Handling Procedure set out in Appendix 6.

OREGON TOOL

# Part II: Our Obligations

This Processor Policy applies in all situations where a Group Member Processes Personal Information as a Processor anywhere in the world. All Team Members and Group Members must comply with the following obligations:

| | |
|---|---|
| **Rule 1 – Lawfulness:**<br><br>***We must ensure that Processing is at all times compliant with applicable law and this Processor Policy.*** | We must at all times comply with any Applicable Data Protection Laws, as well as the standards set out in this Processor Policy, when Processing Personal Information.<br><br>As such:<br>• where Applicable Data Protection Laws exceed the standards set out in this Processor Policy, and thus require a higher level of protection for Personal Information than this Processor Policy, we must comply with those laws; but<br>• where there are no Applicable Data Protection Laws, or where Applicable Data Protection Laws do not meet the standards set out in this Processor Policy, we must Process Personal Information in accordance with the standards set out in this Processor Policy. |
| **Rule 2 – Cooperation with Customers:**<br><br>***We must cooperate with and assist the Customer to comply with its obligations under Applicable Data Protection Laws in a reasonable time and to the extent reasonably possible.*** | We must cooperate with and assist our Customer to comply with its obligations under Applicable Date Protection Laws. We must provide such assistance in a reasonable time and to the extent reasonably possible, whether the Group Member is Processing the Personal Information as a Processor or a sub-Processor, and as required under the terms of our contract with the Customer.<br><br>Assistance may include, for example, helping our Customer to keep the Personal Information we Process on its behalf accurate and up to date, helping it to provide individuals with access to their Personal Information, or helping it to conduct data protection impact assessments in accordance with Applicable Data Protection Laws. |
| **Rule 3 – Fairness and Transparency:**<br><br>***We must, to the extent reasonably possible, assist a Customer to comply with the requirement to explain to individuals how their Personal Information will be Processed.*** | Our Customer has a duty to explain to the individuals whose Personal Information it Processes (or instructs us to Process), how and why that Personal Information will be used. This information must be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language.<br><br>This is usually done by means of an easily accessible fair Processing statement. We will provide such assistance and information to the Customer in accordance with the terms of our contract with the Customer to comply with this requirement.<br><br>For example, the terms of our contract with a Customer may require us to provide information about any Sub-Processors we appoint to Process Personal Information on our Customer's behalf. |

| | |
|---|---|
| **Rule 4 – Purpose Limitation:**<br><br>***We will only Process Personal Information on behalf of and in accordance with the instructions of the Customer.*** | We must only Process Personal Information on behalf of the Customer and in accordance with its documented instructions (for example, as set out in the terms of our contract with the Customer), including with regard to any international transfers of Personal Information, unless we are otherwise required to do so by Union or Member State law to which we are subject. In such a case, we shall inform the Customer of that legal requirement before Processing takes place, unless that law prohibits such information on important grounds of public interest. If in our opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions, we shall immediately inform the Customer.<br><br>If we are unable to comply with our Customer's instructions (or any of our obligations under this Processor Policy), we will inform the Customer promptly. The Customer may then suspend its transfer of Personal Information to us and/or terminate its contract with us (in accordance with the terms of the contract).<br><br>In such circumstances or more generally upon termination of the provision of services related to the Processing, we will return or delete the Personal Information, including any copies of the Personal Information, in a secure manner or as otherwise required, whether we are acting as a Processor or as a sub-Processor, in accordance with the terms of our contract with the Customer and certify to the Customer that this has been done.<br><br>If we are prevented from returning the Personal Information to our Customer or from deleting it (for example, due to applicable law requirements), we must inform the Customer. In such event, we must continue to maintain the confidentiality of the Personal Information and not Process the Personal Information further other than in accordance with the terms of our contract with the Customer. |
| **Rule 5 – Data Accuracy and Minimisation**<br><br>***We will assist our Customer to keep the Personal Information accurate and up to date.*** | We must assist our Customer to comply with its obligation to keep Personal Information accurate and up to date. In particular, where a Customer informs us that Personal Information is inaccurate, we must assist our Customer to update, correct or erase the Personal Information without delay.<br><br>We must also take measures to inform Group Members or third-party Processors to whom the Personal Information has been disclosed of the need to update, correct or erase the Personal Information. |
| **Rule 6 – Storage Limitation:**<br><br>***We will assist our Customer to store Personal Information only for as long as is necessary for the purpose for which*** | Where a Customer instructs us that Personal Information we Process on its behalf is no longer needed for the purposes for which it was collected, we will assist our Customer to erase, restrict or anonymise the Personal Information without delay and in accordance with the terms of our contract with the Customer. |

| | |
|---|---|
| ***the information was initially collected.*** | We must also take measures to inform Group Members or third-party Processors to whom the Personal Information has been disclosed of the need to erase, restrict or anonymise the Personal Information. |
| **Rule 7 – Security, Integrity and Confidentiality:**<br><br>***We must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the Personal Information we Process on behalf of a Customer.*** | Where we provide a service to a Customer which involves the Processing of Personal Information, the contract between us and that Customer will set out the technical and organisational security measures we must implement to safeguard the Personal Information consistent with Applicable Data Protection Laws.<br><br>We must ensure that any Team Member who has access to Personal Information Processed on behalf of a Customer does so only for purposes that are consistent with the Customer's instructions and is subject to a duty of confidentiality. |
| **Rule 8 – Accountability:**<br><br>***We must be able to demonstrate compliance with this Processor Policy and Applicable Data Protection Laws.*** | Taking into account the nature, scope, context and purposes of Processing as well as any potential risks to the rights and freedoms of individuals whose Personal Information we Process, we must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that we Process Personal Information in accordance with this Processor Policy and with Applicable Data Protection Laws. We must review those measures and update them where necessary.<br><br>We also have a duty to make available to the Controller all information necessary to demonstrate our compliance with our obligations as a Processor. |
| **Rule 9 – Security Incident Reporting:**<br><br>***We must notify a Customer of any security incident that we experience if it presents a risk to the Personal Information we Process on the Customer's behalf.*** | When we become aware of a data security incident that may affect the Personal Information that we Process on behalf of a Customer, we must immediately inform the Incident Response Team.<br><br>The Incident Response Team will review the nature of the data security incident and determine whether it is necessary to notify a Customer. The Group DPO shall be responsible for ensuring that any such notifications, where necessary, are made without undue delay and in accordance with applicable law.<br><br>Where applicable, we will assist the Customer to comply with its obligations as set out in Articles 32 to 36 of the GDPR, taking into account the nature of processing and information available to us. |
| **Rule 10 – Engaging Sub-Processors**<br><br>***We may only appoint, add or replace Sub-Processors with authorisation from*** | We must obtain a Customer's authorisation before appointing, adding or replacing a Sub-Processor to Process Personal Information on its behalf, regardless of whether this Sub-Processor is a Group Member or not. Authorisation must be obtained in accordance with the terms of our contract with the Customer. |

| | |
|---|---|
| ***the Customer and in accordance with its requirements.*** | We must make available to our Customer up-to-date information about the Sub-Processors (both internal and external) we intend to appoint in order to obtain its authorisation. If, on reviewing this information, a Customer objects to the appointment of a Sub-Processor, that Customer may take such steps as are consistent with the terms of its contract with us and as referred to in Rule 4 of this Processor Policy regarding the return or destruction of the Personal Information. |
| | We must only appoint Sub-Processors (whether internal or external) who provide sufficient guarantees in respect of the commitments made by us in this Processor Policy. In particular, Sub-Processors must implement appropriate technical and organisational security measures to protect the Personal Information they Process, and such measures must be consistent with our commitments to our Customer under our contractual terms with the Customer. |
| **Rule 11 – Sub-Processor Contracts**<br><br>***We must only appoint Sub-Processors who protect Personal Information to a standard that is consistent with this Processor Policy and our contractual terms with Customers.*** | Where we intend to appoint an internal or an external Sub-Processor to Process Personal Information, we must undertake due diligence to ensure it has in place appropriate technical and organisational security measures to protect the Personal Information. We must impose strict contractual obligations in writing and require that it:<br>• protect the Personal Information to a standard that is consistent with our commitments to our Customer under the terms of our contract with the Customer;<br>• maintain the security of the Personal Information, consistent with standards contained in this Processor Policy (and in particular Rules 7, 8 and 9 above);<br>• Process Personal Information only on our instructions (consistent with the instructions of the Customer) or on the Customer's instructions; and<br>• fulfill such additional obligations as may be necessary to ensure that the commitments made by the Sub-Processor reflect those made by us in this Processor Policy and provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals regarding any international transfers of Personal Information (including any onward transfers of Personal Information). |
| **Rule 12 – Respect for Individuals' Data Protection Rights:**<br><br>***We will assist a Customer to respond to queries or requests made by individuals in connection with their Personal Information.*** | We must assist our Customer to comply with its duty to respect the data protection rights of individuals, in accordance with the instructions of our Customer and the terms of our contract with the Customer.<br><br>In particular, if any Group Member receives a request from any individual wishing to exercise his or her data protection rights regarding Personal Information for which the Customer is the Controller, the Group Member must transfer such request promptly to the relevant Customer and not respond to such a request unless authorised to do so or required by law. |

| | |
|---|---|
| **Rule 13 – Privacy by Design and Default:**<br><br>***We must provide our products and services in a way that assists our Customer to apply data protection by design and by default principles.*** | We must provide our products and services in a way that assists our Customer to implement Privacy by Design and Privacy by Default principles. This means that we must implement appropriate technical and organizational measures when providing our products and services that:<br>• are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards in order to protect the rights of individuals and meet the requirements of Applicable Data Protection Laws ("**Privacy by Design**"); and<br>• ensure that, by default, only Personal Information which are necessary for each specific Processing purpose are collected, stored, Processed and are accessible; in particular, that by default Personal Information is not made accessible to an indefinite number of people without the individual's intervention ("**Privacy by Default**").<br><br>These measures must be implemented in accordance with the terms of our agreement with our Customer. |

OREGON TOOL

# Part III: Delivering Compliance in Practice

To ensure we follow the rules set out in our Processor Policy, in particular, the obligations set out in Part II, Oregon Tool and its Group Members must also comply with the following practical commitments:

| | |
|---|---|
| **1. Resourcing and Compliance:**<br><br>***We must have appropriate Team Members and support to ensure and oversee privacy compliance throughout the business.*** | Oregon Tool has appointed a Group DPO with the support of the Privacy Team to oversee and ensure compliance with this Processor Policy. The Group DPO with support from the Privacy Team is responsible for overseeing and enabling compliance with this Processor Policy on a day-to-day basis.<br><br>The Group DPO receives the support of the highest management within Oregon Tool. The Group DPO reports directly to Oregon Tool's Board of Directors on all material or strategic issues relating to Oregon Tool's compliance with Applicable Data Protection Laws and the Processor Policy and the Group DPO is also accountable to Oregon Tool's independent audit committee.<br><br>A more detailed overview of the roles and responsibilities of Oregon Tool's Group DPO and Privacy Team is set out in Appendix 3. |
| **2. Privacy Training:**<br><br>***We must ensure Team Members are educated about the need to protect Personal Information in accordance with this Processor Policy.*** | Group Members must provide appropriate privacy training to Team Members who:<br>• have permanent or regular access to Personal Information; or<br>• are involved in the Processing of Personal Information or in the development of tools used to Process Personal Information.<br><br>We will provide such training in accordance with the Privacy Training Program (see Appendix 4). |
| **3. Records of Data Processing:**<br><br>***We must maintain records of the Processing activities carried out on behalf of a Customer.*** | We must maintain a record of the Processing activities that we conduct on behalf of a Customer in accordance with Applicable Data Protection Laws. These records should be kept in writing (including electronic form) and we must make these records available to competent data protection authorities upon request. Further details about the records of processing are provided in Appendix 11.<br><br>The Group DPO with the support of the Privacy Team is responsible for ensuring that such records are maintained. |
| **4. Audit:**<br><br>***We must have data protection audits on a regular basis.*** | We will have data protection audits on a regular basis, which may be conducted by either internal or external accredited auditors. In addition, we will conduct data protection audits as requested from the Internal Audit Team. Such audits will cover all aspects of this Processor Policy (including methods of ensuring that corrective actions will take place). |

| | |
|---|---|
| | The Customer may also audit us (or any Sub-Processors acting on our behalf) to ensure we comply with our obligations under this Processor Policy in respect of the Processing we carry out on behalf of Customer, in accordance with the terms of Customer's contract with us.<br><br>We will conduct any such audits in accordance with the Audit Protocol (see Appendix 5), which includes providing a copy of the data protection reports to the Group DPO and the Board of Directors' Audit Committee and to the Data Protection Authorities upon request. The Data Protection Authorities may audit Group Members for compliance with the Processor Policy (including any related procedures and controls) in accordance with our Cooperation Procedure (see Appendix 7). |
| **5. Complaint Handling**<br><br>***We must enable individuals to raise data protection complaints and concerns.*** | Group Members must enable individuals to raise data protection complaints and concerns (including complaints about Processing under this Processor Policy) with Oregon Tool's Privacy Team, with the Data Protection Authorities or with the competent national courts, by complying with the Complaint Handling Procedure (see Appendix 6). In particular, individuals may contact Oregon Tool's Privacy Team at privacy@oregontool.com who will respond without undue delay and in any event within one month, unless an extension of two additional months is needed by Oregon Tool, taking into account the complexity and number of the requests. |
| **6. Cooperation with the Data Protection Authorities:**<br><br>***We must always cooperate with the Data Protection Authorities.*** | Group Members must cooperate with the Data Protection Authorities for the Controller by complying with the Cooperation Procedure (see Appendix 7) and will abide by a formal decision of any Data Protection Authority on any issues relating to the interpretation and application of the Processor Policy. Group Members may appeal any formal decision of any Data Protection Authority in accordance with the laws of the country in which the Data Protection Authority is established. |
| **7. Updates to this Processor Policy:**<br><br>***We will update this Processor Policy in accordance with our Updating Procedure.*** | Whenever updating our Processor Policy, we must comply with the Updating Procedure (see Appendix 8). |
| **8. Conflicts Between this Processor Policy and National Legislation:**<br><br>***We must take care where local laws conflict with this Policy, and act responsibly to ensure a high standard or protection for*** | If local laws applicable to any Group Member may prevent it from fulfilling its obligations under the Processor Policy or under the contract with the Customer or otherwise has a substantial effect on its ability to comply with the Processor Policy or the instructions it has received from a Customer, the Group Member must promptly inform:<br>• Oregon Tool Europe SA;<br>• the Customer (consistent with the requirements of Rule 4); |

| | |
|---|---|
| ***the Personal Information in such circumstances.*** | • the Group DPO;<br>• the Data Protection Authority for the Customer; and<br>• the Data Protection Authority for the Group Member;<br><br>unless otherwise prohibited by law. |
| **9. Government Requests for Disclosure of Personal Information:**<br><br>***We must notify the Data Protection Authorities in case of a legally binding request for disclosure of Personal Information.*** | If a Group Member receives a legally binding request for disclosure of Personal Information by a law enforcement authority or state security body which is subject to this Processor Policy, it must:<br>• notify the Customer promptly unless prohibited from doing so by applicable law; and<br>• comply with the requirements of its Government Data Request Procedure set out in Appendix 9.<br><br>In no event shall transfers of Personal Information from any Group Member to any law enforcement, state security or other government authority be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society. |

OREGON TOOL

# Part IV: Third-Party Beneficiary Rights

## A. Scope of the third-party beneficiary rights

This Part IV applies where individuals' Personal Information are protected under the data protection laws of the EEA (including the General Data Protection Regulation). This is the case when:

- an individuals' Personal Information are Processed in the context of the activities of a third-party Controller or a Group Member (acting as a Processor) established in the EEA;
- a non-EEA Customer (acting as a Controller) or Group Member (acting as a Processor) offers goods and services (including free goods and services) to those individuals in the EEA; or
- a non-EEA Customer (acting as a Controller) or Group Member (acting as a Processor) monitors the behaviour of the individuals, as far as their behaviour takes place in the EEA;

and the Customer or Group Member (as applicable) then transfers those individuals' Personal Information to a non-EEA Group Member (or its Sub-Processor) for Processing under the Processor Policy.

Under Applicable Data Protection Laws, individuals whose Personal Information is Processed in the EEA by a Group Member acting as a Processor (an "**EEA Entity**") and/or transferred to a Group Member located outside Europe under the Processor Policy (a "**Non-EEA Entity**") have certain rights. These rights also exist where a Non-EEA Entity Group Member acting as a Processor receives Personal Information under the Processor Policy from a Controller located within the EEA.

The principles that individuals may enforce as third-party beneficiaries are those that are set out under:

- Part I-G (Introduction) of this Processor Policy;
- Part II (Our Obligations) of this Processor Policy;
- Part III (Delivering Compliance in Practice) of this Processor Policy, including paragraphs 5 (Complaint Handling), 6 (Cooperation with the Data Protection Authorities), 8 (Conflicts Between this Processor Policy and National Legislation) and 9 (Government Requests for Disclosure of Personal Information);
- Part IV (Third-Party Beneficiary Rights) of this Processor Policy; and
- the corresponding Appendices that are referenced in each of the relevant sections mentioned above.

These individuals may directly enforce the Processor Policy as third-party beneficiaries, and they may also directly enforce the Processor Policy as third-party beneficiaries where they cannot bring a claim against a Controller in respect of non-compliance of any of the commitments in this Processor Policy by a Group Member (or by a sub-processor) acting as a Processor because:

(a) the Controller has factually disappeared or ceased to exist in law or has become insolvent; and

(b) no successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law.

In such cases, individuals may exercise the following rights:

- *Complaints*: Individuals may complain to a Group Member and/or to a Data Protection Authority, in accordance with the Complaint Handling Procedure (Appendix 6);
- *Proceedings*: Individuals may commence proceedings against a Group Member for violations of this Processor Policy, in accordance the Complaint Handling Procedure (Appendix 6);
- *Compensation*: Individuals who have suffered material or non-material damage as the result of an infringement of this Processor Policy have the right to receive compensation from Oregon Tool for the damage suffered.
- *Transparency*: Individuals also have the right to obtain a copy of this Processor Policy upon request by contacting the Group DPO at privacy@oregontool.com or by visiting www.oregontool.com.

**B. Responsibility for breaches by non-EEA Group Members**

OREGON TOOL EUROPE SA will be responsible for ensuring that any action necessary is taken to remedy any breach of this Processor Policy by a non-EEA Group Member (or any non-EEA Sub-Processor appointed by a Group Member) in accordance with the Complaint Handling Procedure (Appendix 6).

In particular:

- If an individual can demonstrate damage he or she has suffered likely occurred because of a breach of this Processor Policy by a non-EEA Group Member (or a non-EEA Sub-Processor appointed by a Group Member), OREGON TOOL EUROPE SA will have the burden of proof to show that the non-EEA Group Member (or non-EEA Sub-Processor) is not responsible for the breach, or that no such breach took place;
- where a non-EEA Group Member (or any non-EEA third party Sub-Processor acting on behalf of a Group Member) fails to comply with this Processor Policy, the courts in the EEA and the Data Protection Authorities will have jurisdiction and individuals may exercise their rights and remedies above against OREGON TOOL EUROPE SA as if the breach of this Processor Policy had been caused by OREGON TOOL EUROPE SA. In this context, individuals may, where appropriate, receive compensation (as determined by a competent court or Data Protection Authorities) from OREGON TOOL EUROPE SA for any material or non-material damage suffered as a result of a breach of this Processor Policy.

### C. Shared liability for breaches with Controllers

Where Oregon Tool is engaged by a Customer to Process Personal Information on its behalf, and both are responsible for harm caused by the Processing in breach of this Processor Policy, Oregon Tool accepts that both Oregon Tool and the Customer may be held liable for the entire damage in order to ensure effective compensation of the individual.

OREGON TOOL

# Part V: Appendices

**APPENDIX 1: LIST OF GROUP MEMBERS**

**APPENDIX 2: DATA PROTECTION RIGHTS PROCEDURE**

**APPENDIX 3: PRIVACY COMPLIANCE STRUCTURE**

**APPENDIX 4: PRIVACY TRAINING PROGRAM**

**APPENDIX 5: AUDIT PROTOCOL**

**APPENDIX 6: COMPLAINT HANDLING PROCEDURE**

**APPENDIX 7: COOPERATION PROCEDURE**

**APPENDIX 8: UPDATING PROCEDURE**

**APPENDIX 9: GOVERNMENT DATA REQUEST PROCEDURE**

**APPENDIX 10: MATERIAL SCOPE OF THE PROCESSOR POLICY**