OREGON TOOL

Binding Corporate Rules:

Controller Policy

OREGON TOOL

Contents

OREGON TOOL

Part I: Introduction

This Binding Corporate Rules: Controller Policy ("**Controller Policy**") establishes Oregon Tool, Inc. and its affiliates' ("**Oregon Tool**") approach to compliance with Applicable Data Protection Laws (in particular, the laws in the EEA) when Processing Personal Information for its own purposes as a Controller.

A. Scope of this Controller Policy

This Controller Policy applies when we Process Personal Information as a Controller and transfer Personal Information between Group Members. This Controller Policy applies regardless of whether our Group Members Process Personal Information by manual or automated means.

The standards described in this Controller Policy are worldwide standards that apply to all Group Members when Processing any Personal Information as a Controller. As such, this Controller 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 Controller Policy

This Controller Policy applies to all Personal Information that we Process as a Controller, including Personal Information that is Processed in the course of our business activities, employment administration and vendor management – such as:

- **Human Resources ("HR") data:** including Personal Information of past and current employees, individual consultants, independent contractors, temporary staff and job applicants;
- **Customer Relationship Management ("CRM") data:** including Personal Information relating to representatives of business customers who use our business services;
- **Supply chain management data:** including Personal Information of individual contractors and of account managers and staff of third-party suppliers who provide services to us; and
- **Website visitors' data:** including Personal Information of individuals who visit, use or register on our websites.

Additional details on the material scope of this Controller Policy are provided in Appendix 11.

C. Our collective responsibility to comply with this Controller Policy

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

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

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

D. 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 Controller 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 Controller Policy.

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

E. Relationship with Oregon Tool's Binding Corporate Rules: Processor Policy

This Controller Policy applies only to Personal Information that Oregon Tool Processes as a Controller (i.e. for its own purposes).

Oregon Tool has a separate Binding Corporate Rules: Processor Policy ("**Processor Policy**") that applies when it Processes Personal Information as a Processor in order to provide a service to a third party (such as a customer).

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 Controller Policy and also with the Processor 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.

F. Where this Controller Policy is made available

OREGON TOOL

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

G. Important terms used in this Controller Policy

For the purposes of this Controller Policy:

- the term **Applicable Data Protection Laws** includes the data protection laws in force in the territory from which a Group Member initially transfers Personal Information under this Controller Policy. Where an EEA Group Member transfers Personal Information under this Controller Policy to a non-EEA Group Member, the term Applicable Data Protection Laws shall include the data protection laws applicable to that Group Member in the EEA (including the European Union's General Data Protection Regulation or "GDPR");
- the term **Controller** means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information. For example, Oregon Tool is a Controller of its HR records and CRM records;
- 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, a third-party service provider that is Processing Personal Information in order to provide a service to Oregon Tool);
- 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 Controller Policy.

H. How to raise questions or concerns

If you have any questions regarding this Controller Policy, your rights under this Controller 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 5, Rue Emile Francqui 1435 Mont-Saint-Guibert Belgium

Attention:	Privacy Team
Email:	privacy@oregontool.com
Address:	Oregon Tool, Inc. 4909 SE International Way, 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 individuals whose Personal Information is Processed by Oregon Tool in accordance with Appendix 9.

If you want to exercise any of your data protection rights, please see the data protection rights procedure set out in Appendix 3. 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 7.

OREGON TOOL

Part II: Our Obligations

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

Rule 1 – Lawfulness: ***We must ensure that Processing is at all times compliant with applicable law and this Controller Policy.***	We must at all times comply with any Applicable Data Protection Laws, as well as the standards set out in this Controller Policy, when Processing Personal Information. As such: • where Applicable Data Protection Laws exceed the standards set out in this Controller Policy, and thus require a higher level of protection for Personal Information than this Controller Policy, we must comply with those laws; but • where there are no Applicable Data Protection Laws, or where Applicable Data Protection Laws do not meet the standards set out in this Controller Policy, we must Process Personal Information in accordance with the standards set out in this Controller Policy.
Rule 2 – Fairness and Transparency: ***We must inform individuals how and why their Personal Information will be Processed.***	We must provide individuals with the Fair Information Disclosures (see Appendix 2) when we Process their Personal Information, in accordance with Applicable Data Protection Laws and in particular with Articles 13 and 14 of the GDPR. We must take appropriate measures to communicate the Fair Information Disclosures to individuals in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The Fair Information Disclosures shall be provided in writing, or by other means, including, where appropriate, by electronic means. They may be provided orally, at the request of an individual, provided that the identity of that individual is proven by other means. If we have not obtained Personal Information directly from the individual him or herself then, in certain limited cases, we may not need to provide the Fair Information Disclosures, as explained in Appendix 2. Where this is the case, the Group DPO and the Privacy Team must be informed and will decide what course of action is appropriate to protect the individual's rights, freedoms and legitimate interests.

	We must only Process Personal Information for specified, explicit and legitimate purposes that have been communicated to the individuals concerned in accordance with Rule 2. We must not Process their Personal Information in a way that is incompatible for those purposes, except in accordance with applicable law or with the individual's consent.
Rule 3 – Purpose Limitation: ***We must Process Personal Information only for specified, explicit and legitimate purposes and not further Process the information in a manner that is incompatible with those purposes.***	If we intend to Process Personal Information for a purpose that is incompatible with the purpose for which the Personal Information was originally collected, then we may only do so if such further Processing is permitted by applicable law or we have the individual's consent. We must also provide the individual with Fair Information Disclosures about the further Processing in accordance with Rule 2. In assessing whether any Processing is compatible with the purpose for which the Personal Information was originally collected, we must take into account: • any **link** between the purposes for which the Personal Information was originally collected and the purposes of the intended further Processing; • the **context** in which the Personal Information was collected, and in particular the reasonable expectations of the individuals whose Personal Information will be Processed; • the **nature** of the Personal Information, in particular whether such information may constitute Sensitive Personal Information; • the **possible consequences** of the intended further Processing for the individuals concerned; and • the existence of any **appropriate safeguards** that we have implemented in both the original and intended further Processing operations.
Rule 4 – Data Minimisation ***We must only Process Personal Information that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.***	We must only Process Personal Information that is adequate, relevant and limited in order to properly fulfill the desired Processing purpose(s). We must not Process Personal Information that is unnecessary to achieve the purpose(s).
Rule 5 – Accuracy: ***We must keep Personal Information accurate and, where necessary, up to date.***	We must take appropriate measures to ensure that the Personal Information we Process is accurate and, where necessary, kept up to date – for example, by giving individuals the ability to inform us when their Personal Information has changed or become inaccurate. We must take every reasonable step to ensure that Personal Information that is inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.

Rule 6 – Storage Limitation: ***We will only keep Personal Information for as long as is necessary for the purposes for which it is collected and further Processed.***	We must not keep Personal Information in a format that permits the identification of individuals for longer than is necessary for the purposes for which the information is Processed. In particular, we must comply with the Oregon Tool's record retention policies and guidelines as revised and updated from time to time.
Rule 7 – Security, Integrity and Confidentiality: ***We must implement appropriate technical and organisational measures to ensure a level of security of Personal Information that is appropriate to the risk for the rights and freedoms of the individuals.***	We must implement appropriate technical and organisational measures to protect Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where Processing involves transmission of Personal Information over a network, and against all other unlawful forms of Processing. In particular, we must comply with the requirements in the security policies in place within Oregon Tool, as revised and updated from time to time, together with any other security procedures relevant to a business area or function. We must ensure that any Team Member who has access to or is involved in the Processing of Personal Information does so only on instructions from Oregon Tool and under a duty of confidentiality.
Rule 8 – Accountability: ***We must be able to demonstrate compliance with this Controller 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 Controller Policy and with Applicable Data Protection Laws. We must review those measures and update them where necessary.
Rule 9 – Service Provider Management: ***We must ensure that our service providers also adopt appropriate security measures when Processing Personal Information.***	Where we appoint an internal or external service provider to Process Personal Information on our behalf (e.g., a Processor), we must impose strict contractual terms on the service provider that require it: • to act only on our instructions when Processing that information, including with regard to international transfers of Personal Information; • to ensure that any individuals who have access to the Personal Information are subject to a duty of confidentiality; • to have in place appropriate technical and organisational security measures to safeguard the Personal Information; • only to engage a sub-Processor if we have given our prior specific or general written authorisation, and on condition the sub-Processor agreement protects the Personal Information to the same standard required of the service provider; • to assist us in ensuring compliance with our obligations as a Controller under Applicable Data Protection Laws, in particular

	with respect to reporting data security incidents under Rule 10 and responding to requests from individuals to exercise their data protection rights under Rule 11; • to return or delete the Personal Information once it has completed its services; and • to make available to us all information we may need in order to ensure its compliance with these obligations.
Rule 10 – Security Incident Reporting: ***We must comply with any data security incident reporting requirements that exist under applicable law.***	When we become aware of a data security incident that presents a risk to the Personal Information that we Process, we must immediately inform the Incident Response Team and follow our Incident Response Policy. The Incident Response Team will review the nature of the data security incident and determine whether it is necessary under Applicable Data Protection Laws: • to notify competent data protection authorities, because the incident is likely to create a **risk** for the rights and freedoms of individuals affected by the incident; and/or • to notify individuals affected by the incident because the incident creates a **high risk** for their rights and freedoms. The Incident Response Team will document all data security incidents (including the facts relating to such incident, its effects and the remedial action taken). The documentation will be made available to the competent data protection authorities on request. The Group DPO shall be responsible for ensuring that any such notifications, where necessary, are made in accordance with the requirements of, and timescales specified by, Applicable Data Protection Laws, which in the case of the GDPR will mean notifying the Data Protection Authorities without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the incident. Where notification to the affected individuals is also required, they must be notified without undue delay.
	Various data protection laws around the world, including the laws in the EEA, provide individuals with certain data protection rights. These may include: • ***The right of access****:* This is a right for an individual to obtain confirmation whether we Process Personal Information about them and, if so, to be provided with details of that Personal Information and access to it; • ***The right to rectification (correction)****:* This is a right for an individual to obtain rectification without undue delay of inaccurate Personal Information we may Process about him or her. • ***The right to erasure****:* This is a right for an individual to require us to erase Personal Information about them on certain grounds

Rule 11 – Respect for Individuals' Data Protection Rights:

We must enable individuals to exercise their data protection rights in accordance with applicable law.

– for example, where the Personal Information is no longer necessary to fulfill the purposes for which it was collected. If we have made the Personal Information public, then (taking account of available technology and the cost of implementation) we must also take reasonable steps, including technical measures, to inform Controllers that are Processing the Personal Information that the individual has requested the erasure by such Controllers of any links to, or copy or replication of, that Personal Information.

- ***The right to restriction****:* This is a right for an individual to require us to restrict Processing of Personal Information about them on certain grounds.
- ***The right to data portability****:* This is a right for an individual to receive Personal Information concerning him or her from us in a structured, commonly used and machine-readable format and to transmit that information to another Controller, if certain grounds apply. Where technically feasible, this may include direct transmission from Oregon Tool to another Controller.
- ***The right to object****:* This is a right for an individual to object, on grounds relating to his or her particular situation, to Processing of personal data about him or her, if certain grounds apply.

Where an individual wishes to exercise any of its data protection rights, we must respect those rights in accordance with applicable law by following the Data Protection Rights Procedure (see Appendix 3).

In addition, the relevant Oregon Tool Group Member shall communicate any rectification or erasure of Personal Information or restriction of Processing carried out in accordance with this rule to each recipient to whom the Personal Information have been disclosed, unless this proves impossible or involves disproportionate effort. We must inform the individual about those recipients if the individual requests it.

Rule 12 – Ensuring Adequate Protection for International Transfers:

We must not transfer Personal Information internationally without ensuring adequate protection for the information in accordance with applicable law.

Various data protection laws around the world, including the laws in the EEA, prohibit international transfers of Personal Information to third countries unless appropriate safeguards are implemented to ensure the transferred data remains protected to the standard required in the country or region from which it is transferred.

Where these requirements exist, we must comply with them. Whenever transferring Personal Information internationally, the Group DPO must be consulted so that they can ensure appropriate safeguards, such as standard contractual clauses (for transfers of Personal Information from the EEA) have been implemented to protect the Personal Information being transferred.

No Group Member may transfer Personal Information internationally unless and until such measures as are necessary to comply with Applicable Data Protection Laws governing international transfers of Personal Information have been satisfied in full.

	For the avoidance of doubt, this Rule 12 also pertains to onward transfers of Personal Information to controllers and processors that are not Group Members.
Rule 13 – Sensitive Personal Information: ***We must only Process Sensitive Personal Information collected in the EEA where we have obtained the individual's explicit consent, unless there is an alternative legitimate basis for Processing consistent with applicable law.***	Oregon Tool will assess whether Sensitive Personal Information is required for the intended purpose of Processing before collecting it. In principle, we must obtain the individual's explicit consent to collect and Process his or her Sensitive Personal Information, unless we are required to do so by applicable law or have another legitimate basis for doing so consistent with the applicable law of the country in which the Personal Information was collected. When obtaining an individual's consent, the consent must be given freely, and must be specific, informed and unambiguous.
Rule 14 – Direct Marketing: ***We must allow customers to opt-out of receiving marketing information.***	All individuals have the right to object, in an easy-to-exercise manner and free of charge, to the use of their Personal Information for direct marketing purposes and we will honour all such opt-out requests.
Rule 15 – Automated Individual Decision-Making, Including Profiling: ***We must respect individuals' rights not to be subject to a decision based solely on automated Processing, including profiling, that produces legal effects or similarly significantly affects them.***	We will not make any decision, which produces legal effects concerning an individual or that similarly significantly affects him or her, based solely on the automated Processing of that individual's Personal Information, including profiling, unless such decision is: • necessary for entering into, or performing, a contract between a Group Member and that individual; • authorized by applicable law (which, in the case of Personal Information about individuals in the EEA, must be European Union or Member State law); • or based on the individual's explicit consent. In the first and third cases above, we must implement suitable measures to protect the individual's rights and freedoms and legitimate interests, including the right to obtain human intervention, to express his or her view and to contest the decision. We must never make automated individual decisions about individuals using their Sensitive Personal Information unless they have given explicit consent under Rule 12 or another lawful basis applies.
Rule 16 – Privacy by Design and Privacy by Default ***We must apply data protection by design and by default principles when designing and***	When designing and implementing new products and systems that Process personal data, we must apply Privacy by Design and Privacy by Default principles. This means we must implement appropriate technical and organisational measures that: • are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards in

implementing new products and systems.	order to protect the rights of individuals and meet the requirements of Applicable Data Protection Laws ("**Privacy by Design**"); and • 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**").

OREGON TOOL

Part III: Delivering Compliance in Practice

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

1. Resourcing and Compliance: ***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 Controller Policy. The Group DPO with support from the Privacy Team is responsible for overseeing and enabling compliance with this Controller Policy on a day-to-day basis. 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 Controller Policy and the Group DPO is also accountable to Oregon Tool's independent audit committee. A more detailed overview of the roles and responsibilities of Oregon Tool's Group DPO and Privacy Team is set out in Appendix 4.
2. Privacy Training: ***We must ensure Team Members are educated about the need to protect Personal Information in accordance with this Controller Policy.***	Group Members must provide appropriate privacy training to Team Members who: • have permanent or regular access to Personal Information; or • are involved in the Processing of Personal Information or in the development of tools used to Process Personal Information. We will provide such training in accordance with the Privacy Training Program (see Appendix 5).
3. Records of Data Processing: ***We must maintain records of the Processing activities under our responsibility.***	We must maintain a record of the Processing activities that we conduct in accordance with Applicable Data Protection Laws. These records should be kept in writing (which may electronic form) and we must make these records available to competent data protection authorities upon request. The Group DPO with the support of the Privacy Team is responsible for ensuring that such records are maintained.
4. Audit: ***We must have data protection audits on 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 on specific request from the Internal Audit Team. Such audits will cover all aspects of this Controller Policy (including methods of ensuring that corrective actions will take place).

	We will conduct any such audits in accordance with the Audit Protocol (see Appendix 6), which includes providing a copy of the data protection reports to the Group DPO and to the data controller's 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 Controller Policy (including any related procedures and controls) in accordance with our Cooperation Procedure (see Appendix 8).
5. Data Protection Impact Assessments: ***We must carry out data protection impact assessments where Processing is likely to result in a high risk to the rights and freedoms of individuals, and consult with competent data protection authorities where required by applicable law.***	Where required by Applicable Data Protection Laws, we must carry out Data Protection Impact Assessments (DPIA) whenever the Processing of Personal Information, particularly using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. Oregon Tool will carry out a DPIA prior to Processing which will contain at least the following: • A systematic **description** of the envisaged Processing operations and the purposes of the Processing; • An assessment of the **necessity and proportionality** of the Processing operations in relation to the purposes; • An assessment of the **risks** to the privacy rights of individuals; • The **measures envisaged** to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Information and demonstrate compliance with Applicable Data Protection Laws. Where the DPIA indicates that the Processing would still result in a high risk to individuals, Oregon Tool will consult with Data Protection Authorities where required by Applicable Data Protection Laws.
6. Complaint Handling: ***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 Controller 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 7). 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.
7. Cooperation with the Data Protection Authorities: ***We must always cooperate with the Data Protection Authorities.***	Group Members must cooperate with the Data Protection Authorities by complying with the Cooperation Procedure (see Appendix 8) and will abide by a formal decision of any Data Protection Authorities on any issues relating to the interpretation and application of the Controller Policy (notwithstanding Oregon Tool's right to appeal any

	such decision and to exercise such right of appeal in accordance with applicable laws).
8. Updates to this Controller Policy: ***We will update this Controller Policy in accordance with our Updating Procedure.***	Whenever updating our Controller Policy, we must comply with the Updating Procedure (see Appendix 9).
9. Conflicts Between this Controller Policy and National Legislation: ***We must take care where local laws conflict with this Policy, and act responsibly to ensure a high standard or protection for the Personal Information in such circumstances.***	If local laws applicable to any Group Member may prevent it from fulfilling its obligations under the Controller Policy or otherwise have a substantial effect on its ability to comply with the Controller Policy, the Group Member must promptly inform: • Oregon Tool Europe SA; and • the Group DPO unless prohibited by a law enforcement authority. The Group DPO will make a responsible decision on the action to take and will, where appropriate; report to the competent data protection authority.
10. Government Requests for Disclosure of Personal Information: ***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 that is subject to this Controller Policy, it must comply with the Government Data Request Procedure set out in Appendix 10. In no event shall transfers of Personal Information from any Group Member transfer Personal Information to any law enforcement, state security or other government authority in a massive, disproportionate and indiscriminate manner that goes 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 Group Member (or its third-party Processor) established in the EEA;
- a non-EEA Group Member (or its third-party Processor) offers goods and services (including free goods and services) to those individuals in the EEA; or
- a non-EEA Group Member (or its third-party Processor) monitors the behaviour of those individuals, as far as their behaviour takes place in the EEA;

and the Group Member then transfers those individuals' Personal Information to a non-EEA Group Member for Processing under the Controller Policy.

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

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

- Part I-G (Introduction) of this Controller Policy;
- Parts II (Our Obligations) of this Controller Policy;
- Part III (Delivering Compliance in Practice) of this Controller Policy, including paragraphs 6 (Complaint Handling), 7 (Cooperation with the Data Protection Authorities), 9 (Conflicts Between this Controller Policy and National Legislation) and 10 (Government Requests for Disclosure of Personal Information);
- Part IV (Third-Party Beneficiary Rights) of this Controller Policy; and
- the corresponding Appendices as referenced in the relevant sections mentioned above.

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 7);
- *Proceedings*: Individuals may commence proceedings against a Group Member for violations of this Controller Policy, in accordance the Complaint Handling Procedure (Appendix 7);

- *Compensation*: Individuals who have suffered material or non-material damage as the result of an infringement of this Controller 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 Controller 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 Controller Policy by a non-EEA Group Member in accordance with the Complaint Handling Procedure (Appendix 7).

In particular:

- If an individual can demonstrate damage he or she has suffered likely occurred because of a breach of this Controller Policy by a non-EEA Group Member, OREGON TOOL EUROPE SA will have the burden of proof to show that the non-EEA Group Member is not responsible for the breach, or that no such breach took place;
- where a non-EEA Group Member fails to comply with this Controller 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 Controller 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 Controller Policy.

OREGON TOOL

Part V: Appendices

APPENDIX 1: LIST OF GROUP MEMBERS

APPENDIX 2: FAIR INFORMATION DISCLOSURES

APPENDIX 3: DATA PROTECTION RIGHTS PROCEDURE

APPENDIX 4: PRIVACY COMPLIANCE STRUCTURE

APPENDIX 5: PRIVACY TRAINING PROGRAM

APPENDIX 6: AUDIT PROTOCOL

APPENDIX 7: COMPLAINT HANDLING PROCEDURE

APPENDIX 8: COOPERATION PROCEDURE

APPENDIX 9: UPDATING PROCEDURE

APPENDIX 10: GOVERNMENT DATA REQUEST PROCEDURE

APPENDIX 11: MATERIAL SCOPE OF THE CONTROLLER POLICY