Binding Corporate Rules:

Processor Policy

Contents

Part I: Introduction to this Processor Policy

What does this Processor Policy do?

This Binding Corporate Rules: Processor Policy ("**Processor Policy**") establishes VMware's approach to compliance with applicable data protection laws when processing personal information on behalf of a third party controller.

It applies in particular when we process personal information as a processor and either: (a) we transfer personal information between members of our group of companies listed in Appendix 1 ("**Group Members**"); or (b) a third party controller transfers personal information to a Group Member for processing. It applies regardless of whether our Group Members process personal information by manual or automated means. For this Processor Policy to apply it must be expressly referenced within the terms of our contract with a controller.

The standards described in the Processor Policy are worldwide standards that apply to all Group Members when processing any personal information as a processor. When we refer in this Processor Policy (or any of its appendices) to a requirement that applies to VMware, or a right that may be exercised against VMware, then that right or requirement shall be read as applying to or exercisable against each Group Member that is processing personal information under this Processor Policy. 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.

For an explanation of some of the terms used in this Processor Policy, like "controller", "process", and "personal information", please see the section headed "Important terms used in this Processor Policy" below.

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) provided it has been referenced within the terms of our contract with the controller. As such, it

applies to personal information processed in the course of providing services to a customer or another Group Member – such as:

- Customer content: personal information that our Customers upload or import onto our service offerings for processing on their behalf.
- Customer support data: personal information that our Customers provide to us in connection with a request for technical or other support.

When a Customer transfers personal information to us for processing in accordance with this Processor Policy, this Processor Policy shall be incorporated by reference into the contract with that Customer.

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 controller 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; and
- the related policies and procedures appended in **Part IV** of this Processor Policy.

Responsibility towards the Customer

When VMware process personal information as a processor, the Customer on whose behalf VMware processes Personal Information will have responsibility for complying with the applicable data protection laws that apply to it. As a consequence, the Customer will pass certain data protection obligations on to VMware in its contract appointing VMware as its processor. If VMware fails to comply with the terms of its processor appointment, this may put the Customer in breach of its applicable data protection laws and Customer may initiate

proceedings against the relevant Group Member or against VMware International Limited for the breach, resulting in the payment of compensation or other judicial remedies.

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 Europe, that Customer is responsible for implementing other appropriate safeguards in accordance with applicable data protection laws.

Responsibility towards individuals

In addition, where an individual demonstrates that he or she has suffered damage, and that it is likely that the damage has occurred due to a breach of this Processor Policy (whether by a Group Member or a third party processor appointed by a Group Member), VMware will be responsible for demonstrating that such Group Member is not responsible for the breach, or that no such breach took place. For European Customers, this burden of proof for demonstrating that the Group Member is not responsible for the breach, or that no such breach took place, shall fall to VMware International Limited.

Management commitment and consequences of non-compliance

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

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

In recognition of the gravity of these risks, staff who do not comply with this Processor Policy may be subject to disciplinary action, up to and including dismissal.

Where will this Processor Policy be made available?

This Processor Policy is accessible on VMware's corporate website at www.vmware.com.

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 in which the controller of the personal information is located. Where a Group Member processes personal information on behalf of a European controller under this Processor Policy, the term applicable data protection laws shall include the European data protection laws applicable to that controller;

- 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, VMware is a controller of its HR records and CRM records;

- the term **Customer** refers to the third party controller on whose behalf VMware processes personal information. It includes VMware's third party customers, as well as VMware Group Members, when we process personal information on their behalf in the course of providing data processing services to them.

- the term **Europe** 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 VMware'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 personal 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 nature personal;

- the term **processing** 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, VMware is a processor of the personal information it processes to provide services to its Customers;

- the term **Processor Policy** refers to this Binding Corporate Rules: Processor Policy. The Processor Policy applies where VMware processes personal information as a processor on behalf of a third party;

- the term **staff** refers to all employees (including new hires and temporary staff) and individual contractors engaged by any VMware Group Member who have permanent or regular access to personal information or who are involved in the collection of personal information or the development of tools used to process personal information.

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 can contact VMware's Privacy Team at privacy@vmware.com. VMware's Privacy Team will either deal with the matter directly or forward it to the appropriate person or department within VMware to respond.

VMware's Privacy Team is responsible for ensuring that changes to this Policy are notified to the Group Members and to Customers whose personal information is processed by VMware in accordance with Appendix 7.

If you are unhappy about the way in which VMware has used your personal information, you can raise a complaint in accordance with our complaint handling procedure set out in Appendix 6.

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 staff 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 Processor Policy.***	We must at all times comply with any applicable data protection laws (including processor obligations under EU Regulation 2016/679 (the General Data Protection Regulation), when applicable), as well as the standards set out in this Processor Policy, when processing personal information. As such: • where applicable data protection laws exceed the standards set out in this Processor 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 Processor Policy, we must process personal information in accordance with the standards set out in this Processor Policy.
Rule 2 – Cooperation with controllers: ***We must cooperate and assist the Customer to comply with***	We must assist our Customer to comply with its obligations under applicable data protection laws. We must provide such assistance within a reasonable time and as required under the terms of our contract with the Customer.

its obligations under applicable data protection laws in a reasonable time and to the extent reasonably possible.	Assistance may include, for example, helping our Customer to keep the personal information we process on its behalf accurate and up to date, or helping it to provide individuals with access to their personal information.
Rule 3 – Fairness and transparency: ***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 information it processes (or instructs us to process), how and why that information will be used. This information must be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language. 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. 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: ***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 instructions (for example, as set out in the terms of our contract with the Customer). 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. In such circumstances, we will return, destroy or store the personal information, including any copies of the personal information, in a secure manner or as otherwise required, in accordance with the terms of our contract with the Customer. If legislation prevents us from returning the personal information to our Customer, or from destroying it, we will maintain the confidentiality of the personal information and will 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: ***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 that information without undue delay and in accordance with the terms of our contract with the Customer. Where a Customer instructs that personal information we process on its behalf is no longer needed for the purposes for which it was collected, we must assist our customer to erase, restrict or anonymise that personal information without undue delay and in accordance with the terms of our contract with the Customer.

Rule 6 – Security and confidentiality: ***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 that information consistent with applicable data protection laws. We must ensure that any staff 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 confidence.
Rule 7 – Security incident reporting: ***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 presents a risk to the personal information that we process on behalf of a Customer, we must immediately inform VMware's Incident Response Team and follow our incident response management procedure and policies. The Incident Response Team will investigate the nature and seriousness of the data security incident and report its findings to the Privacy Team. The Privacy Team shall take into account the Incident Response Team's findings and applicable law to determine whether it is necessary to notify a Customer. We must ensure that any such notifications, where necessary, are made without undue delay and in accordance with applicable law.

Rule 8 – Engaging sub-processors ***We may only appoint, add or replace sub-processors with authorisation from the Customer and in accordance with its requirements.***	We must obtain a Customer's authorisation before appointing, adding or replacing a sub-processor to process personal information on its behalf. Authorisation must be obtained in accordance with the terms of our contract with the Customer. We must make available to our Customer up-to-date information about the sub-processors we intend to appoint in order to obtain its authorisation. If, on reviewing this information, a Customer reasonably objects for reasons relating to data protection to the appointment of a sub-processor, that Customer may take such steps as are consistent with the terms of its contract with us.
Rule 9 – Sub-processor contracts ***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.***	We must only appoint sub-processors 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. Where we intend to appoint a 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 on the sub-processor that require it: • to 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; • to maintain the security of the personal information, consistent with standards contained in this Processor Policy (and in particular Rules 6, 7 and 8 above); • to process personal information only on our instructions (which instructions will be consistent with the instructions of the Customer) on the Customer's instructions, or as necessary to comply with applicable data protection laws; and • to fulfil 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 which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals in respect of any international transfers of personal information.
Rule 10 – Respect for individuals' data protection rights: ***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. In particular, if any Group Member receives a request from any individual wishing to exercise his or her data protection rights in respect of 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. We will provide the Customer with assistance to fulfil the request in accordance with the terms of our contract with the Customer.
Rule 11 – Third Party Beneficiary Rights in Europe: ***We must provide individuals with easy access to this Processor Policy, including information about their third party beneficiary rights.***	Under European data protection law, individuals whose personal information is processed in Europe 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 individuals may enforce the Processor Policy as third party beneficiaries where they cannot bring a claim against a Customer in respect of a breach of any of the commitments in this Processor Policy by a Group Member (or by a sub-processor) acting as a Processor because: (i) the Customer has factually disappeared or ceased to exist in law or has become insolvent; and (ii) no successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law. In such cases, the individual's rights are as follows: (a) *Complaints*: Individuals may complain to an EEA Entity in accordance with the Complaint Handling Procedure. They may also complain to: (i) the data protection authority in Ireland (where VMware's European headquarters is located); (ii) the European data protection authority in the jurisdiction of the transferring EEA Entity; or (iii) if neither (i) or (ii) are possible, the data protection authority of the EEA

Member State where the individual resides;

(b) *Proceedings:* Individuals may bring proceedings against VMware International Limited before the courts in:

(i) Ireland;

(ii) the jurisdiction from which the personal information was transferred; or

(iii) if (i) or (ii) are not possible, the jurisdiction of the EEA Member State where the individual resides;

(c) *Compensation:* Individuals may seek appropriate redress from VMware International Limited (including the remedy of any breach of the Processor Policy by a Non-EEA Entity) and where appropriate, receive compensation from VMware International Limited for any damage suffered as a result of a breach of this Processor Policy by:

(i) a Non-EEA Entity; or

(ii) any third party processor which is established outside the EEA and which is acting on behalf of an EEA Entity or a Non-EEA Entity; or

(iii) in accordance with the determination of the court or other competent authority;

(d) *Transparency:* Individuals may obtain a copy of this Processor Policy and the Intra-group Agreement entered into by VMware in connection with this Processor Policy from VMware or any other EEA Entity upon request.

Where a Non-EEA Entity acts as a Processor on behalf of a third party controller, then if an individual suffers damage and where that individual can demonstrate that it is likely that the damage has occurred because of a breach of this Processor Policy, the burden of proof to show that (i) a Non-EEA Entity; or (ii) any third party sub-processor who is established outside the EEA who is acting on behalf of a Non-EEA Entity is not responsible for the breach, or that no such breach took place, will rest with VMware International Limited.

VMware International Limited will ensure that any action necessary is taken to remedy any breach of the Processor Policy by a Non-EEA Entity or any third party processor which is established outside the EEA and which is processing personal information on behalf of a Customer.

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, VMware and all of its Group Members must also comply with the following practical commitments:

Resourcing and compliance:

We must have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

VMware has appointed its Privacy Team to oversee VMware's compliance with applicable data protection laws and this Processor Policy. The Privacy Team is responsible for overseeing and enabling compliance on a day-to-day basis.

The Privacy Team reports to the VP, Chief Ethics & Compliance Officer, who in turn reports to the General Counsel and the Board of Directors. The VP, Chief Ethics & Compliance Officer reports on VMware's privacy efforts and the status of its privacy program to the audit committee of the Board of Directors.

In addition to the Privacy Team, VMware has also established the following data protection roles and responsibilities:

(a) VMware Master Data Management Information Governance Executive Council: VMware has established an executive council that comprises key stakeholders across various global departments, including functional departments responsible for cloud services delivery and customer support and various regional offices (including VMware's offices in the EEA). The council meets on a regular basis to discuss the overall direction and strategy of VMware's data practices, as well as to consider

	evolving legal, regulatory or operational data protection issues. VMware's Privacy Team participates in meetings of the council, and reports any material issues arising from these meetings to VMware's VP, Chief Ethics & Compliance Officer. (b) *Regional Ethics & Compliance Officers*: VMware has compliance officers placed across various local offices worldwide. These compliance officers serve as the on-the-ground presence for local employees on data protection and other compliance-related matters, and act as local liaison points for the Privacy Team. They escalate local privacy issues to the Privacy Team and also assist with the flow down to their regions privacy awareness-raising and advice as needed. (c) *Employee reporting*: VMware encourages all of its employees to report issues of privacy non-compliance upwards through their line management, local human resources personnel, Privacy Committee stakeholders or directly the Privacy Team. Employees may also report concerns about privacy non-compliance directly to VMware's VP, Chief Ethics & Compliance Officer.
Privacy training: ***We must ensure staff are educated about the need to protect personal information in accordance with this Processor***	Group Members must provide appropriate privacy training to staff members who: • have permanent or regular access to personal information; or • are involved in the processing of personal

Policy	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 2).
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 Privacy Team or the Board of Directors. We will conduct any such audits in accordance with the Audit Protocol (see Appendix 3).
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 about this Processor Policy by complying with the Complaint Handling Procedure (see Appendix 4).
Cooperation with competent data protection authorities: ***We must always cooperate with competent data protection authorities***	Group Members must cooperate with competent data protection authorities by complying with the Cooperation Procedure (see Appendix 5)
Conflicts between this Processor Policy and national legislation:	If legislation applicable to any Group Member prevents it from fulfilling its obligations under the Processor Policy or otherwise has a substantial effect on its ability to comply with the Processor Policy, the Group Member must promptly

	inform: • the Customer (consistent with the requirements of Rule 4); • the Privacy Team ; and • the appropriate data protection authority competent for the Customer; unless otherwise prohibited by law.
Government requests for disclosure of personal information:	If a Group Member receives a legally binding request for disclosure of personal information which is subject to this Processor Policy, it must: • notify the Customer promptly unless prohibited from doing so by a law enforcement authority; and • use its best efforts to put the request on hold and notify the appropriate data protection authority competent for the Customer by complying with the requirements of its Government Data Request Procedure set out in Appendix 6. Where VMware is not in a position to notify the competent data protection authority of the request, VMware commits to preparing an annual Transparency Report and to make this Transparency Report available upon request to competent data protection authorities, in accordance with the Government Data Request Procedure set out in Appendix 6.
Updates to this Processor Policy:	Whenever updating our Processor Policy, we must comply with the Updating Procedure (see Appendix 7).

Part IV: Related policies and procedures

APPENDIX 1

VMWARE GROUP MEMBERS

APPENDIX 2

PRIVACY TRAINING PROGRAM

APPENDIX 3

AUDIT PROTOCOL

APPENDIX 4

COMPLAINT HANDLING PROCEDURE

APPENDIX 5

CO-OPERATION PROCEDURE

APPENDIX 6

GOVERNMENT DATA REQUEST PROCEDURE

APPENDIX 7

UPDATING PROCEDURE