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. However, we must apply the standards described in this Processor Policy to all transfers of personal information to and between Group Members, even if they are not explicitly listed above.

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;

- the third party beneficiary rights set out in **Part IV**; and

- the related policies and procedures appended in **Part V** of this Processor Policy.

Responsibility towards the Customer

As a data processor, VMware will have a number of direct legal obligations under applicable data protection laws that apply to it. In addition, however, the Customer will also 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 Unlimited Company 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-European Group Member (or a non-European third party processor appointed by a Group

Member) processes personal information for which the Customer is a controller in breach of this Processor Policy, that Customer may enforce the Processor Policy against VMware International Unlimited Company. In such event, VMware International Unlimited Company 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 is incorporated into the contract with that Customer. The contract confirms that VMware (and any other Group Member or sub-processor) will process all personal information from Europe on behalf of the Customer in accordance with the Processor Policy 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.

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 supervisory 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 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 (including Regulation 2016/679 (**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, 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** (and **European**) 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 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 **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. All staff must comply with this Processor Policy.

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 including the GDPR 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 4.

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.

The rights and obligations that apply to personal information within the scope of this Processor Policy "travel" with the personal information whenever it is transferred to or between Group Members (or their sub-processors). This means that where in-scope personal information is transferred to an importing Group Member (or its sub-processor) in another country, that personal information must be protected to the standards set out in this Processor Policy, even if the importing Group Member (or its sub-processor) is not subject to applicable data protection laws or is subject to applicable data protection laws that provide for lower standards.

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 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 data protection laws including the GDPR. We must provide such assistance within a reasonable time and as required under the terms of our contract with the Customer. 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, or providing relevant information to Customer to enable Customer to conduct data protection impact assessments in accordance with applicable data protection laws.
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***	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

accordance with the instructions of, the Customer.	Customer), including with regard to any international transfers of personal information. 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 and, if requested, certify to the Customer that this has been done. If we are prevented from returning the personal information to our Customer, or from destroying 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 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. We must also take measures to inform Group Member or third party processors to whom the personal information has been disclosed of the need to update, correct or erase that personal information.
Rule 6 – Storage limitation: ***We will assist our Customer to store personal information only for as long as is necessary for the purpose for which the information was initially collected.***	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 that personal information without delay and in accordance with the terms of our contract with the Customer. 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 that personal information.
Rule 7 – Security, integrity 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 8 – Security incident reporting: ***We must notify a Customer of any security incident that we***	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

experience if it presents a risk to the personal information we process on the Customer's behalf.	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 9 – 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 prior informed specific or general authorisation before appointing, adding or replacing a sub-processor (whether Group Members or not) 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 any sub-processor we intend to appoint or replace in a timely manner in order to obtain the Customer's authorisation before any personal information is disclosed to the sub-processor. 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 and as referred to in Rule 4 of this Processor Policy regarding the return or destruction of the personal information, which includes the option for the Customer to terminate the contract.
Rule 10 – Sub-processor contracts	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

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.	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 provide sufficient guarantees to implement appropriate technical and organisational measures to ensure the processing will meet the requirements of applicable data protection laws; • to maintain the security of the personal information, consistent with standards contained in this Processor Policy (and in particular Rules 7, 8 and 9 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; • to ensure that any onward transfers of personal information to other sub-processors (whether Group Members or other third party sub-processors) are permitted only with the Customer's prior informed specific or general authorization, consistent with the requirements of Rule 9 (Engaging Sub-processors); 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 11 – 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 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 data protection laws.**	Wherever we transfer personal information internationally, we must ensure an adequate level of protection for the personal information in accordance with applicable data protection laws. In some transfer circumstances where personal information is transferred to a Group Member by a Customer, either under applicable law and/or pursuant to the contract between us and that Customer, the Customer may also have commitments to ensure security and to protect personal information – for example, by the Customer taking steps to sufficiently configure the technical solution. This includes transfers of personal

	information to Group Members that are subject to this Processor Policy and transfers (and onward transfers) from Group Members to third parties that are not subject to this Processor Policy. We must also comply with our Customers' documented instructions in respect of any international transfers of personal information (as described in Rule 4). Where a Group Member makes an international transfer of personal information that is subject to the GDPR from Europe to another Group Member or third party located in a third country, a territory or one or more specified sectors within that third country that does not provide an adequate level of protection ("**Non-Adequate Location**"), we must: • undertake a risk assessment ("**Transfer Impact Assessment**") to assess whether there is reason to believe that the laws and practices in the Non-Adequate Location, including any requirements to disclose personal information to public authorities or measures that authorise access by public authorities, will conflict with VMware's obligations under this Processor Policy; and • where the Transfer Impact Assessment concludes that additional safeguards are necessary to ensure an adequate level of protection for the personal information and compliance with this Processor Policy, implement such additional safeguards (if appropriate, in consultation with the Controller). Where a Group Member located in Non-Adequate Location receives personal information that is subject to the GDPR from another Group Member or third party, that Group Member must promptly notify the transferring Group Member or third party if it has reason to believe that it is or has become subject

	to laws or practices not in line with the requirements of this Processor Policy, including following a change in the laws of the Non-Adequate Location. We will conduct such Transfer Impact Assessments and promptly notify any transfer risks in accordance with the Transfer Impact Assessment Procedure (see Appendix 8).

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:

---

1. 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 with this Processor Policy on a day-to-day basis.

The Privacy Team reports to the Chief Privacy Officer, who in turn reports to the General Counsel and the Board of Directors. The Chief Privacy 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 Privacy Governance Councils 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 Chief Privacy Officer.

	(b) Compliance officers and *regional lawyers* VMware has compliance officers and regional lawyers placed across various local offices worldwide. These officers/lawyers 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, or directly to the Privacy Team. Employees may also report concerns about privacy non-compliance directly to VMware's VP, Chief Ethics and Compliance Officer.
2. Privacy training: ***We must ensure staff are educated about the need to protect personal information in accordance with this Processor Policy***	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 information or in the development of tools used to process personal information. We will provide such training in accordance with the Privacy Training Requirements (see Appendix 2).
3. Records of Data Processing:	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

We must maintain records of the data processing activities carried out on behalf of a Customer.	(including electronic form) and we must make these records available to competent supervisory authorities upon request. VMware's 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 Privacy Team or the Board of Directors. We will conduct any such audits in accordance with the Audit Protocol (see Appendix 3).
5. Data protection by design and by default ***We must provide our services in a way that assists our Customer to apply data protection by design and by default principles.***	We must provide our services in a way that assists our Customer to implement data protection by design and data protection by default principles. This means that we must implement appropriate technical and organizational measures when providing our services that: • 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 • ensure that, by default, only personal data which are necessary for each specific processing purpose are collected, stored, processed and are accessible; in particular, that by default personal data is not made accessible to an indefinite number of people without the individual's intervention ("**privacy by default**").

	These measures must be implemented in accordance with the terms of our agreement with our Customer.
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 Processor Policy) by complying with the Complaint Handling Procedure (see Appendix 4).
7. Cooperation with supervisory authorities: ***We must always cooperate with supervisory authorities***	Group Members must cooperate with supervisory authorities by complying with the Cooperation Procedure (see Appendix 5).
8. Conflicts between this Processor 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 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, or the instructions it has received from a Customer, the Group Member must promptly inform: • the Customer (consistent with the requirements of Rule 4); • the Privacy Team; and • the competent supervisory authority for the Customer; and • the competent supervisory authority for the Group Member, unless otherwise prohibited by law. When undertaking a transfer of personal information to a Non-Adequate Country, Group Members must comply with the

	requirements of Rule 12 of Part II of this Processor Policy, to minimise the likelihood and risk of any such conflict arising in the first place.
9. Government requests for disclosure of personal information: ***We must notify the competent supervisory 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 which is subject to this Processor Policy by a law enforcement authority or state security body, 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 supervisory 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 supervisory authority of the request, VMware commits to preparing an annual Disclosure Overview and to make this Disclosure Overview available upon request to competent supervisory authorities, in accordance with the Government Data Request Procedure set out in Appendix 6. In no event must transfers of personal information from a Group Member to any law enforcement, state security or similar public authority be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.
10. Updates to this Processor Policy:	Whenever updating our Processor Policy, we must comply with the Updating Procedure (see Appendix 7).

We will update this Processor Policy in accordance with our Updating Procedure.

Part IV: Third Party Beneficiary Rights

Application of this Part IV

This Part IV applies where individuals' personal information are protected under European data protection laws (including the General Data Protection Regulation). This is the case when:

- those individuals' personal information are processed in the context of the activities of a third-party controller or a Group Member (acting as processor) established in Europe;
- a non-European Customer (acting as controller) or Group Member (acting as processor) offers goods and services (including free goods and services) to those individuals in Europe; or
- a non-European Customer (acting as controller) or Group Member (acting as processor) monitors the behaviour of those individuals, as far as their behaviour takes place in Europe;

and that Customer or Group Member (as applicable) then transfers those individuals' personal information to a non-European Group Member (or its sub-processor) for processing under the Processor Policy.

Entitlement to effective remedies

When this Part IV applies, individuals have the right to pursue effective remedies in the event their personal information is processed by VMware in breach of the following provisions of this Processor Policy:

- Part II (Our Obligations) of this Processor Policy;
- Paragraphs 6 (Complaint Handling), 7 (Cooperation with supervisory authorities), 8 (Conflicts between this Processor Policy and national legislation) and 9 (Government requests for disclosure of personal information) under Part III of this Processor Policy; and
- Part IV (Third Party Beneficiary Rights) of this Processor Policy.

Individuals' third party beneficiary rights

When this Part IV applies, the right for individuals to pursue effective remedies against VMware apply only if either (i) the requirements at stake are specifically directed at VMware as a processor in accordance with applicable data protection law including the GDPR (and in accordance with guidance

published by competent supervisory authorities), or (ii) the individuals cannot bring a claim against a Customer because:

- the Customer has factually disappeared or ceased to exist in law or has become insolvent; and
- no successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law.

In the case of (i) above, individuals may exercise the following rights:

- VMware's duty to respect the instructions of the controller (including those involving data transfers);
- VMware's duty to cooperate and assist the controller to comply with and demonstrate compliance with the law (including data subject rights requests);
- VMware's duty to implement appropriate technical and organisational measures and to notify any data security incident to the relevant controller in line with Rule 8;
- VMware's duty to engage sub-processors (whether Group Members or not) in line with Rules 9 and 10;
- those contained in any local law preventing respect of BCRs; and
- those listed immediately below.

In the case of (ii) above, individuals may exercise the following rights:

- *Complaints*: Individuals may complain to a Group Member and/or to a European supervisory authority, in accordance with the Complaint Handling Procedure at Appendix 4;
- *Proceedings*: Individuals may commence proceedings against a Group Member for violations of this Processor Policy, in accordance the Complaint Handling Procedure at Appendix 4;
- *Compensation*: Individuals who have suffered material or non-material damage as a result of an infringement of this Processor Policy have the right to receive compensation from VMware for the damage suffered; and
- *Transparency*: Individuals also have the right to obtain a copy of the Processor Policy on request to Privacy Team at privacy@vmware.com.

Responsibility for breaches by non-European Group Members

VMware International Unlimited Company will be responsible for ensuring that any action necessary is taken to remedy any breach of the Processor Policy by a non-European Group Member (or any non-European sub-processor appointed by a Group Member).

In particular:

- if an individual can demonstrate damage it has suffered likely occurred because of a breach of this Processor Policy by a non-European Group Member (or a non-European sub-processor appointed by a Group Member), VMware International Unlimited Company will have the burden of proof to show that the non-European Group Member (or non-European sub-processor) is not responsible for the breach, or that no such breach took place; and

- where a non-European Group Member (or any non-European third party sub-processor acting on behalf of a Group Member) fails to comply with this Processor Policy, individuals may exercise their rights and remedies above against VMware International Unlimited Company and, where appropriate, receive compensation (as determined by a competent court or other competent authority) from VMware International Unlimited Company for any material or non-material damage suffered as a result of a breach of this Processor Policy;

Shared liability for breaches with controllers

Where VMware is engaged by a Customer to conduct processing and both are responsible for harm caused by the processing in breach of this Processor Policy, VMware accepts that both VMware and the Customer may be held liable for the entire damage in order to ensure effective compensation of the individual.

Part V: Related policies and procedures

APPENDIX 1

VMWARE LIST OF GROUP MEMBERS

VMware – EEA Entities

The EEA Entities are as follows:

Name of entity	Registered address	Email Address
Austria		
VMware Marketing Austria GmbH	Business Embassy. Sky 360, Operngasse 17-21, Bena Sky, Vienna, 1040, Austria	dpo@vmware.com
Bulgaria		
VMware Bulgaria EOOD	16A, G.M. Dimitrov Blvd., Sofia, 1797, Bulgaria	dpo@vmware.com
Denmark		
VMware Denmark ApS	Linde Alle 9, Nærum, DK-2850, Denmark	dpo@vmware.com
France		
VMware France SAS	Tour Franklin, 100-101 Terrasse Boieldieu, Paris, 92042, France	dpo@vmware.com
Italy		
VMware Italy S.r.l	Via Giovanni Spadolini 5/7 Torre A, Milano, 20141, Italy	dpo@vmware.com
Ireland		

VMware Bermuda Unlimited Company	70 Sir John Rogerson's Quay. Dublin 2, Ireland	dpo@vmware.com
VMware International Unlimited Company	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland.	dpo@vmware.com
VMware International Marketing Limited	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland	dpo@vmware.com
Netherlands		
VMware Netherlands B.V.	Orteliuslaan 850, Nieuwegein, Utrecht, 3528 BB, Netherlands	dpo@vmware.com
Spain		
VMware Spain, S.L.	Calle Rafael Boti 26, 2nd Floor, Madrid, 28023, Spain	dpo@vmware.com
Sweden		
VMware Sweden AB	Gustav III's Boulevard 54-58, Solna, 69 74 , Sweden	dpo@vmware.com

VMware – Non-EEA Entities

The Non-EEA Entities are as follows:

Name of entity	Registered address	Email Address
Armenia		
VMware Eastern Europe	22 Hanrapeutyan Street, Suite 5, Yerevan, 0010, Armenia	privacy@vmware.com
Australia		
VMware Australia Pty Ltd	L8, 175 Pitt Street, Sydney, New South Wales, 2000, Australia	dpo@vmware.com
Brazil		
VMware Software e Serviços Brasil Ltda.	Rua Surubim, 504 3rd and 4th floors, suites 32,41,42, Cidade Monções, San Paolo, 04571-050, Brazil	dpo@vmware.com
Canada		
VMware Canada ULC.	c/o Deloitte Legal Canada LLP 1500-885 West Georgia Street Vancouver BC V6C 3EB Canada	dpo@vmware.com
China		
VMware Information Technology (China) Co, Ltd	Room 308-312, Level 8, 17, 18, So. Wing of Tower C, Raycom InfoTech Park, 2 Kexueyuan South Road, Haidian District, Beijing, China 100190	dpo@vmware.com
Costa Rica		

VMware Costa Rica Ltda.	600m N de Plaza Real Cariari, Zona Franca America, Edificio F32, San Francisco, Heredia, Costa Rica	dpo@vmware.com
Dubai		
VMware Middle East FZ-LLC	702A-704A 7th Floor, Business Central Tower A, Dubai Internet City, Dubai, UAE	dpo@vmware.com
Hong Kong		
VMware Hong Kong Limited	Suites 401-02 & 12-14, 4/F Cityplaza 4, 12 Taikoo Wan Rd, Taikoo Shing, Hong Kong	dpo@vmware.com
India		
VMware Software India Private Limited	Kalyani Magnum, Tower 1, 3rd Floor. Doraisanipalya, IIM Post, Bannergha Road, Bangalore, Karnakata-KS, 560076, India	dpo@vmware.com
Israel		
VMware Israel Ltd	Ampa Building, 3 Sapir Street, POB 125, Tel Aviv, Israel, 46733	dpo@vmware.com
Japan		
VMware, K.K.	13F Hamamatsucho Square, 1-30-5, Hamamatsucho, Minato-ku, Tokyo 105-0013, Japan	dpo@vmware.com
Korea		
VMware Korea Co Ltd	Samsung-Dong, ASEM Tower, 13th Floor, 517, Yeongdong-daero, Gangnam-gu, Seoul, 06164, Korea	dpo@vmware.com
Malaysia		

VMware Malaysia SDN. BHD.	Suite 6.01, 6th Floor, Plaza See Hoy Char, Jalan Raja Chulan, Kuala Lumpur Wilayah Persekutuan, 50200 Malaysia	dpo@vmware.com
New Zealand		
VMware NZ Company	Level 19, 157 Lambton Quay, Wellington, 6011, New Zealand	dpo@vmware.com
Singapore		
VMware Singapore Pte Ltd	1 Marina Boulevard, #28-00, Singapore, 018989, Singapore	dpo@vmware.com
Switzerland		
VMware Switzerland GmbH	Hardturmstrasse 181, Zurich, 8005, Switzerland	dpo@vmware.com
Taiwan		
Taiwan VMware Information Technology LLC	The Executive Center, 57th Flr Taipei 101 Tower, 7 Xinyi Road, Taipei, Taiwan	dpo@vmware.com
Thailand		
VMware (Thailand) Co. Ltd	Level 33, Suites No. 3325,3359-3365 Sukhumvit Road, Khwaeng - North Klongtoey, Khet –Wattanam Bangkok Metropolis, 10110, Thailand.	privacy@vmware.com
Turkey		
VMware Turkey Software Solutions	Levent Mah. Büyükdere Cad. Business Towers, Tower 2, Floor: 26 34330,Besiktas, Istanbul, Turkey	privacy@vmware.com

and Services Company Limited		
United Kingdom		
VMware UK Limited	The Pavillions Bridgwater Road, Bristol, BS13 8FD, United Kingdom	wabraham@vmware.com
United States of America		
AirWatch LLC	The Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware, 19801, USA	privacy@vmware.com
A.W.S. Holding, LLC	c/o Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, Delaware 19808, USA	privacy@vmware.com
Carbon Black, LLC	CT Corporation, 1209 Orange Street, Wilmington Delaware 19808, United States	privacy@vmware.com
CloudHealth Technologies, LLC	280 Summer Street, 6th Floor, Boston MA 02210, USA	privacy@vmware.com
Datrium, LLC	3500 S Dupont Hwy, Dover DE, 19901, United States	privacy@vmware.com
Lastline, LLC	251 Little Falls Drive, Wilmington DE 19808, United States (Principal place of business: 3401 Hillview Ave, Palo Alto, California, 94304, USA)	privacy@vmware.com
Nicira Inc	The Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware 19801, USA	privacy@vmware.com
Pivotal Software, Inc	3401 Hillview Ave, Palo Alto, California, 94304, USA	privacy@vmware.com

Velocloud Networks, LLC	3401 Hillview Ave Palo Alto, CA 94304, USA	privacy@vmware.com
VMware Global, Inc	The Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware, 19801, USA	privacy@vmware.com
VMware, Inc.	The Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware, 19801, USA (Principal place of business: 3401 Hillview Ave, Palo Alto, California, 94304, USA)	privacy@vmware.com

APPENDIX 2

PRIVACY TRAINING REQUIREMENTS

1. Background

1.1 The "Binding Corporate Rules: Processor Policy" (the "**Processor Policy**") provides a framework for the transfer of personal information between VMware group members ("**Group Members**"). This document sets out the requirements for VMware to train its staff members on the requirements of the Processor Policy.

1.2 VMware must train staff members on the basic principles of data protection, confidentiality and information security awareness. This must include training on applicable data protection laws, including European data protection laws.

1.3 Certain staff members must receive additional, tailored training on the Processor Policy and specific data protection issues relevant to their role. This training is further described below and is repeated on a regular basis.

2. Responsibility for the Privacy Training Program

2.1 VMware's Ethics & Compliance Team has overall responsibility for privacy training at VMware, with input with colleagues from other functional areas, as appropriate. They will review training from time to time to ensure it addresses all relevant aspects of the Processor Policy.

2.2 VMware's senior management is committed to the delivery of data protection training courses, and will ensure that staff are required to participate, and given appropriate time to attend, such courses. Course attendance must be monitored, for example through VMware's e-learning platforms.

2.3 Instances of persistent non-attendance data protection training courses will be escalated through VMware's internal progressive discipline process for action by VMware's Employee Relations team (working in conjunction with VMware's Ethics & Compliance Team). Such action may include escalation of non-attendance to appropriate managers within VMware who will be responsible and held accountable for ensuring that the individual(s) concerned attend and actively participate in such training.

3. Delivery of the training courses

3.1 VMware will deliver training courses that are designed to be both informative and user-friendly.

3.2 VMware staff members must complete data protection training (including training on the Processor Policy):

(a) as part of their new hire program;

(b) as part of a regular refresher training at least once every two years;

(c) as and when necessary to stay aware of changes in the law; and

(d) as and when necessary to address any compliance issues arising from time to time.

3.3 Certain staff members must receive supplemental specialist training, in particular staff members who work in cloud services delivery and customer support. Specialist training may be tailored as necessary to the course participants.

4. Training on data protection

4.1 VMware's training on data protection and the Processor Policy will cover the following main areas:

4.1.1 Data Protection and the BCRs:

(a) What is data protection law?

(b) What are key data protection terminology and concepts?

(c) What are the data protection principles?

(d) How does data protection law affect VMware internationally?

(e) What are BCRs for Processors?

(f) What are VMware's BCR commitments?

4.1.2 Where relevant to a staff member's role, training will cover the following procedures under the Processor Policy:

(a) Data Subject Rights Procedure

(b) Audit Protocol

(c) Updating Procedure

(d) Cooperation Procedure

(e) Complaint Handling Procedure

(f) Government Data Request Procedure

APPENDIX 3

AUDIT PROTOCOL

1. Background

1.1 VMware's "Binding Corporate Rules: Processor Policy" (the "**Processor Policy**") safeguards personal information transferred between the VMware group members ("**Group Members**").

1.2 VMware must audit its compliance with the Processor Policy on a regular basis, and this document describes how and when VMware must perform such audits. Although this Audit Protocol describes the formal assessment process by which VMware will audit its compliance with the Processor Policy, this is only one way in which VMware ensures that the provisions of the Processor Policy are observed and corrective actions taken as required.

1.3 In particular, VMware's Privacy Team provides ongoing guidance about the processing of personal information and will continually assess the processing of personal information by Group Members for potential privacy-related risks and compliance with the Processor Policy.

2. Conduct of an audit

Overview of audit requirements

2.1 Compliance with the Processor Policy is overseen on a day to day basis by the Privacy Team. The internal audit teams are responsible for performing and/or overseeing independent audits of compliance by VMware's Group Members and business functions with the Processor Policy and will ensure that such audits address all aspects of the Policies as described in Section 2.5.

2.2 The internal audit teams are responsible for ensuring that any issues or instances of non-compliance by VMware Group Members or business functions with the Processor Policy are brought to the attention of the Privacy Team and for recommending where corrective actions must be taken. Serious non-compliance issues will be escalated to the Board of Directors in accordance with paragraph 2.9.

2.3 The Customer (or auditors acting on its behalf) may audit VMware for compliance with the commitments made in the Processor Policy and may extend such audits to any sub-processors

acting on VMware's behalf in respect of such processing. Such audits shall be conducted in accordance with the terms of Customer's contract with VMware.

Frequency of audit

2.4 Audits of compliance with the Processor Policy by VMware Group Members and business functions are conducted:

(a) regularly in accordance with VMware's audit procedures;

(b) at the request of the Privacy Team and / or the Board of Directors (for example, in response to a specific incident); and/or

(c) (with respect to audits of the Processor Policy), as required by the terms of the Customer's contract with VMware.

Scope of audit

2.5 The internal audit teams will determine the scope of an audit following a risk-based analysis that takes into account relevant criteria such as:

(a) areas of current regulatory focus;

(b) areas of specific or new risk for the business;

(c) areas with changes to the systems or processes used to safeguard information;

(d) areas where there have been previous audit findings or complaints;

(e) the period since the last review; and

(f) the nature and location of the personal information processed.

2.6 In the event that a Customer exercises its right to audit VMware for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities, data files and documentation relating to that Customer.

Auditors

2.7 Audit of compliance with the Processor Policy (including any related procedures and controls) by Group Members and business functions will be undertaken by the internal audit teams, or

by independent and experienced professional auditors retained by the internal audit teams, acting under a duty of confidence and in possession of the required professional qualifications, as necessary to perform audits of compliance with the Processor Policy (including any related procedures and controls) relating to data privacy.

2.8 If a Customer exercises its right to audit VMware for compliance with the Processor Policy, such audit may be undertaken by that Customer, or by independent and suitably experienced auditors approved by that Customer, in accordance with the terms of the Customer's contract with VMware.

Reporting

2.9 Results of any audits of compliance with the Processor Policy must be submitted to the Privacy Team and, if the report reveals breaches or the potential for breaches of a serious nature (for example, presenting a risk of potential harm to individuals or to the business), to the Audit Committee (made up of members of the Board of Directors).

2.10 Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, VMware will provide an accurate summary of the results of the most recent data privacy audits of the Processor Policy (including any related procedures and controls):

(a) to competent supervisory authorities; and

(b) to the extent that an audit of compliance with the Processor Policy relates to personal information VMware processes on behalf of a Customer, to that Customer.

2.11 The Privacy Team is responsible for liaising with the competent supervisory authorities for the purpose of providing the information outlined in paragraph 2.10.

Supervisory authority audits

2.12 VMware agrees that competent supervisory authorities may audit Group Members for the purpose of reviewing compliance with the Processor Policy (including any related procedures and controls) in accordance with the Binding Corporate Rules: Cooperation Procedure.

APPENDIX 4

COMPLAINT HANDLING PROCEDURE

1. Background

1.1 VMware's "Binding Corporate Rules: Processor Policy" (the "**Processor Policy**") safeguards personal information transferred between the VMware group members ("**Group Members**").

1.2 This Complaint Handling Procedure describes how complaints brought by an individual whose personal information is processed by VMware under the Processor Policy must be addressed and resolved.

1.3 This procedure will be made available to Customers on whose behalf VMware processes personal information under the Processor Policy.

2. How individuals can bring complaints

2.1 Any individuals may raise a data protection question, concern or complaint in connection with this Processor Policy by e-mailing privacy@vmware.com.

3. Complaints under the Processor Policy

3.1 *Communicating complaints to the Customer*

3.1.1 Where a complaint is brought in respect of the Processor Policy (whereby VMware is processing personal information as a processor on behalf of a Customer), VMware will communicate the details of the complaint to the relevant Customer without undue delay and without handling it (unless VMware) has agreed in the terms of its contract with the Customer to handle complaints).

3.1.2 VMware will provide assistance to the Customer to investigate the complaint, in accordance with the terms of its contract with the Customer and as instructed by the Customer.

3.2 *What happens if a Customer no longer exists?*

3.2.1 In circumstances where a Customer has disappeared, no longer exists or has become insolvent, and no successor entity has taken its place, individuals whose personal information are processed under the Processor Policy have the right to complain to VMware and VMware

will handle such complaints in accordance with paragraph 4 below of this Complaint Handling Procedure.

3.2.2 In such cases, individuals may also have the right to complain to a competent supervisory authority and/or to lodge a claim with a court of competent jurisdiction, including where they are not satisfied with the way in which their complaint has been resolved by VMware. Such complaints and proceedings will be handled in accordance with paragraph 5 below of this Complaint Handling Procedure.

4. Complaints where Customer no longer exists

4.1 *Who handles complaints?*

4.1.1 All questions, concerns, or complaints in respect of the Processor Policy will be handled through the Privacy Team. The Privacy Team will liaise with colleagues from relevant business and support units as necessary to address and resolve such questions, concerns and complaints.

4.2 *What is the response time?*

4.2.1 The Privacy Team will acknowledge receipt of a question, concern or complaint to the individual concerned without undue delay, investigating and making a substantive response within one (1) month.

4.2.2 If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Privacy Team will advise the individual accordingly and provide a reasonable estimate (not exceeding two (2) months) of the timescale within which a substantive response will be provided.

4.3 *What happens if an individual disputes a finding?*

4.3.1 If the individual notifies the Privacy Team that it disputes any aspect of the response finding, the Privacy Team will refer the matter to the Chief Privacy Officer. The Chief Privacy Officer will review the case and advise the individual of his or her decision either to accept the original finding or to substitute a new finding. The Chief Privacy Officer will respond to the complainant within one (1) month from being notified of the escalation of the dispute.

4.3.2 As part of its review, the Chief Privacy Officer may arrange to meet the parties to the dispute to attempt to resolve it. If, due to the complexity of the dispute, a substantive response

cannot be given within one (1) month of its escalation, the Chief Privacy Officer will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided which will not exceed two (2) months from the date the dispute was escalated.

4.3.3 If the complaint is upheld, the Chief Privacy Officer will arrange for any necessary steps to be taken as a consequence.

5. Right to complain to a competent supervisory authority and to commence proceedings

5.1 Where individuals' personal information are processed in Europe by a Group Member acting as a Processor and/or transferred to a Group Member located outside Europe under the Processor Policy then those individuals have certain additional rights to pursue effective remedies for their complaints, as described in paragraphs 5.3 to 5.7 below.

5.2 VMware accepts that complaints and claims made under this Complaint Handling Procedure may be lodged by a non-for-profit body, organisation or association acting on behalf of an individual.

5.3 The individuals described in paragraph 5.1 have the right to complain to a competent supervisory authority (in accordance with paragraphs 5.4 and 5.5) and/or to commence proceedings in a court of competent jurisdiction (in accordance with paragraphs 5.6 and 5.7) in accordance with applicable data protection laws, whether or not they have first complained directly to the Customer or to VMware under this Complaints Handling Procedure.

Complain to a supervisory authority

5.4 If such an individual wishes to complain about VMware's processing of his or her personal information to a supervisory authority on the basis that a European Group Member has processed personal information in breach of the Processor Policy or in breach of applicable data protection laws, he or she may complain to the supervisory authority in the European territory:

(a) of his or her habitual residence;

(b) of his or her place of work; or

(c) where the alleged infringement occurred.

5.5 If an individual wishes to complain about VMware's processing of his or her personal information to a supervisory authority, on the basis that a non-European Group Member has processed personal information in breach of the Processor Policy or in breach of applicable data protection laws, then VMware International Unlimited Company will submit to the jurisdiction of the competent supervisory authority (determined in accordance with paragraph 5.4 above) in place of that non-European Group Member, as if the alleged breach had been caused by VMware International Unlimited Company.

Proceedings before a national court

5.6 If such an individual wishes to commence court proceedings against VMware, on the basis that a European Group Member has processed personal information in breach of the Processor Policy, or in breach of applicable data protection laws, he or she may bring proceedings against that European Group Member in the European territory:

(a) in which that European Group Member is established; or

(b) his or her habitual residence.

5.7 If an individual wishes to commence court proceedings against VMware, on the basis that a non-European Group Member has processed personal information in breach of the Processor Policy or in breach of applicable data protection laws, then VMware International Unlimited Company will submit to the jurisdiction of the competent data court (determined in accordance with paragraph 5.5 above) in place of that non-European group member, as if the alleged breach had been caused by VMware International Unlimited Company.

APPENDIX 5

COOPERATION PROCEDURE

1. Introduction

1.1 This Binding Corporate Rules: Cooperation Procedure sets out the way in which VMware will cooperate with competent supervisory authorities in relation to the "VMware Binding Corporate Rules: Processor Policy" (the "**Processor Policy**").

2. Cooperation Procedure

2.1 Where required, VMware will make the necessary personnel available for dialogue with a competent supervisory authority in relation to the Processor Policy.

2.2 VMware will review, consider and (as appropriate) implement:

(a) any advice or decisions of relevant competent supervisory authorities on any data protection law issues that may affect the Processor Policy; and

(b) any guidance published by supervisory authorities (including the European Data Protection Board) in connection with Binding Corporate Rules for Processors or, where relevant, to Binding Corporate Rules more generally.

2.3 Subject to applicable data protection law and respect for the confidentiality and trade secrets of the information provided, VMware will provide upon request an accurate summary of the results of the most recent audit of the Processor Policy to a competent supervisory authority.

2.4 VMware agrees that a competent supervisory authority may audit any Group Member:

(a) located within its jurisdiction for compliance with the Processor Policy, in accordance with the applicable data protection law(s) of that jurisdiction; and

(b) who processes personal information for a Customer established within the jurisdiction of that supervisory authority for compliance with the Processor Policy, in accordance with the applicable data protection law(s) of that jurisdiction and with full respect to the confidentiality of the information obtained and to the trade secrets of VMware (unless this requirement is in conflict with applicable data protection law).

2.5 VMware agrees to abide by a formal decision of any competent supervisory authority against which a right to appeal is not exercised on any issues relating to the interpretation and application of the Processor Policy.

APPENDIX 6

GOVERNMENT DATA REQUEST PROCEDURE

1. Introduction

1.1 This Binding Corporate Rules: Government Data Request Procedure sets out VMware's procedure for responding to a request received from a law enforcement or other government authority (together the "**Requesting Authority**") to disclose personal information processed by VMware on behalf of a Customer (hereafter "**Data Disclosure Request**").

1.2 Where VMware receives a Data Disclosure Request, it will handle that Data Disclosure Request in accordance with this Procedure.

2. General principle on Data Disclosure Requests

2.1 As a general principle, VMware does not disclose personal information in response to a Data Disclosure Request unless either:

- it is under a compelling legal obligation to make such disclosure; or
- taking into account the nature, context, purposes, scope and urgency of the Data Disclosure Request and the privacy rights and freedoms of any affected individuals, there is an imminent risk of serious harm that merits compliance with the Data Disclosure Requests in any event.

2.2 Even where disclosure is required, VMware's policy is that the Customer should have the opportunity to protect the personal information requested because it has the greatest interest in opposing, or is in the better position to comply with, a Data Disclosure Request.

2.3 For that reason, unless it is legally prohibited from doing so or there is an imminent risk of serious harm, VMware will first notify and cooperate with the competent supervisory authorities and provide the Customer with details of the Data Disclosure Request. VMware will cooperate with the competent supervisory authorities and the Customer to address the Data Disclosure Request.

3. Handling of a Data Disclosure Request

3.1 <u>Receipt of a Data Disclosure Request</u>

3.1.1 If a VMware Group Member receives a Data Disclosure Request, the recipient of the request must pass it to VMware's Vice President, Deputy General Counsel for Litigation immediately upon receipt, indicating the date on which it was received together with any other information which may assist VMware's Vice President, Deputy General Counsel for Litigation to deal with the request. VMware's Vice President, Deputy General Counsel for Litigation will, in turn, promptly inform and consult the Privacy Team about the privacy implications of the Data Disclosure Request and any data protection measures that must be taken.

3.1.2 The request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Disclosure Request. Any Data Disclosure Request, howsoever made, must be notified to Vice President, Deputy General Counsel for Litigation for review.

3.2 Initial steps

3.2.1 VMware's Vice President, Deputy General Counsel for Litigation will carefully review each and every Data Disclosure Request on a case-by-case basis in consultation with the Privacy Team. VMware's Vice President, Deputy General Counsel for Litigation will also liaise with members of the legal department, including the Chief Privacy Officer, as appropriate, to deal with the request to determine the nature, context, purposes, scope and urgency of the Data Disclosure Request, as well as its validity under applicable laws, in order to identify whether action may be needed to challenge the Data Disclosure Request.

4. Notice of a Data Disclosure Request

4.1 Notice to the Customer

4.1.1 After assessing the nature, context, purposes, scope and urgency of the Data Protection Request, VMware will notify and provide the Customer with the details of the Data Disclosure Request prior to disclosing any personal information, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

4.2 Notice to the competent supervisory authorities

4.2.1 VMware will also put the request on hold in order to notify and consult with the competent supervisory authorities, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

4.2.2 Where VMware is prohibited from notifying the competent supervisory authorities and suspending the request, VMware will use its best efforts (taking into account the nature, context, purposes, scope and urgency of the request) to inform the Requesting Authority about its obligations under applicable data protection law and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority to put the request on hold so that VMware can consult with the competent supervisory authorities. VMware will maintain a written record of the efforts it takes.

5. Disclosure Overview

5.1 Where, in the above cases, VMware is not in a position to notify the competent supervisory authorities of the request, VMware commits to preparing an annual report (a "**Disclosure Overview**"), which provides to the extent permitted by applicable laws general information on the requests it has received (e.g. the number and type of Data Disclosure Requests it has received for the preceding year and the Requesting Authorities who made those requests). VMware shall provide this report to the lead supervisory authority which authorized its BCR (and any other competent supervisory authorities that the lead supervisory authority may direct) once a year.

6. Bulk transfers

6.1 In no event will any group member transfer personal information to a Requesting Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

APPENDIX 7

UPDATING PROCEDURE

1. Introduction

1.1 This Binding Corporate Rules: Updating Procedure describes how VMware must communicate changes to the "Binding Corporate Rules: Processor Policy" ("**Processor Policy**") to competent supervisory authorities, individual data subjects, its Customers and to VMware group members ("**Group Members**") bound by the Processor Policy.

1.2 Any reference to VMware in this Updating Procedure is to the Privacy Team which is accountable for ensuring that the commitments made by VMware in this Updating Procedure are met.

2. Records keeping

2.1 VMware must maintain a change log setting out details of each and every revision made to the Processor Policy, including the nature of the revision, the reasons for making the revision, the date the revision was made, and who authorised the revision.

2.2 VMware must also maintain an accurate and up-to-date list of Group Members that are bound by the Processor Policy and of the sub-processors appointed by VMware to process personal information on behalf of Customers. This information must be made available on request from VMware to competent supervisory authorities and to Customers and individuals who benefit from the Processor Policy.

2.3 The Privacy Team shall be responsible for ensuring that the records described in this paragraph 2 are maintained and kept accurate and up-to-date.

3. Changes to the Processor Policy

3.1 All proposed changes to the Processor Policy must be reviewed and approved by Privacy Team in order to ensure that the standards of data protection described in these policies are maintained for the rights of individuals who benefit from them. No changes to the Processor Policy shall take effect unless reviewed and approved by the Privacy Team.

3.2 VMware will communicate all changes to the Processor Policy (including reasons that justify the changes) or to the list of Group Members bound by the Processor Policy:

(a) to the Group Members bound by the Processor Policy via written notice (which may include e-mail or posting on an internal intranet accessible to all Group Members);

(b) systematically to Customers in accordance with the terms of their contracts (and, if any changes are material in nature, they VMware must actively communicate such changes to Customers before they take effect, in accordance with paragraph 4.2 below); and

(c) to the supervisory authority that was the lead authority for the purposes of granting VMware's Processor BCR authorisation (the **"Lead Authority"**) and any other supervisory authorities the Lead Authority may direct at least once a year.

4. Communication of material changes

4.1 If VMware makes any material changes to the Processor Policy or to the list of Group Members bound by the Processor Policy that affect the level of protection offered by the Processor Policy or otherwise affect the Processor Policy (for example by making changes to its binding nature), it will promptly report such changes (including the reasons that justify such changes) to the Lead Authority.

4.2 If a proposed change to the Processor Policy will materially affect VMware's processing of personal information on behalf of a Customer, VMware will also:

(a) actively communicate the proposed change to the affected Customer before it takes effect, and with sufficient notice to enable the affected Customer to raise objections; and

(b) the Customer may then suspend the transfer of personal information to VMware and/or terminate the contract, in accordance with the terms of its contract with VMware.

5. Transfers to new Group Members

5.1 If VMware intends to transfer personal information to any new Group Members under the Processor Policy, it must first ensure that all such new Group Members are bound by the Processor Policy before transferring personal information to them.

APPENDIX 8

TRANSFER IMPACT ASSESSMENT PROCEDURE

1. Introduction

1.1 This Binding Corporate Rules: Transfer Impact Assessment Procedure ("**Transfer Impact Assessment Procedure**") describes how VMware will ensure there is adequate protection for personal information that is subject to the GDPR when it transfers such personal information internationally. It sets out VMware's procedure for conducting transfer impact assessments and promptly notifying any transfer risks in accordance with applicable data protection laws.

1.2 The procedures and evaluations undertaken pursuant to this Transfer Impact Assessment Procedure, in particular those contained in paragraph 3.4, should be conducted based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the Binding Corporate Rules: Processor Policy ("**Processor Policy**").

1.3 Any capitalised terms or expressions used in this Transfer Impact Assessment Procedure have the same meanings given in the Processor Policy.

2. Data transfer compliance

2.1 The GDPR prohibits international transfers of personal information from Europe to a third country, a territory or one or more specified sectors within that third country that do not provide an adequate level of protection ("**Non-Adequate Location**") unless appropriate safeguards are implemented to ensure the transferred data remains protected to the standard required under the GDPR. This includes transfers of personal information to Group Members who are subject to the Processor Policy, and transfers (and onward transfers) from Group Members to third parties who are not subject to the Processor Policy. Where these requirements exist, VMware must comply with them.

2.2 As a Processor, VMware must also comply with our Customers' documented instructions in respect of any international transfers of personal information as set forth in the applicable agreements with Customers.

2.3 Whenever a Group Member transfers personal information to another Group Member for processing in a Non-Adequate Location, or onward transfers personal information to third parties for processing in a Non-Adequate Location, the Privacy Team must be consulted so that they can ensure appropriate safeguards (such as standard contractual clauses) have been implemented to protect the personal information being transferred and, where necessary, a Transfer Impact Assessment has been conducted (as described below in Section 3).

2.4 No Group Member may transfer personal information internationally, or onward transfer personal information, unless and until such measures as are necessary to comply with the Customers' documented instructions, and the requirements under applicable data protection laws governing international or onward transfers of personal information, have been satisfied.

3. Transfer Impact Assessments

3.1 Before a transferring Group Member (a "**Data Transferor**") makes an international transfer (or onward transfer) of personal information that is subject to the GDPR to a recipient Group Member or third-party data recipient (a "**Data Recipient**") located in a Non-Adequate Location, the Data Transferor must coordinate with the Privacy Team to undertake a risk assessment to ensure there is no reason to believe that the laws and practices in the Non-Adequate Location where the Data Recipient will process the personal information, including any requirements to disclose personal information to public authorities or measures authorising access by public authorities (a "**Transfer Impact Assessment**"), will conflict with VMware's obligations under the Processor Policy .

3.2 The Privacy Team shall liaise with the Data Transferor and Data Recipient as necessary to conduct the Transfer Impact Assessment, and shall coordinate with VMware International Unlimited Company as the responsible party in the EEA under the Processor Policy to keep it informed of the Transfer Impact Assessment and its findings.

Requirements for international data transfers

3.3 No international transfer (or onward transfer) of personal information may take place unless and until:

i. a Transfer Impact Assessment has been conducted; and

ii. any additional safeguards identified as necessary pursuant to the Transfer Impact Assessment to protect the transfer of personal information to the Data Recipient have been implemented by the Data Transferor and Data Recipient.

Factors to consider for Transfer Impact Assessments

3.4 The Transfer Impact Assessment should consider the following elements as applicable:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used, any intended onward transfers, the type of recipient, the purpose of processing, the categories and format of the transferred personal information, the economic sector in which the transfer occurs, and the storage location of the data transferred;

ii. the laws and practices of the Non-Adequate Location where Data Recipient transfers and processes personal data (including those requiring the disclosure of data to public authorities or authorising access by such authorities, and those providing for access to these data during the transit between the country of the Data Exporter and the country of the Data Importer), relevant considering the specific circumstances of the transfer and the applicable limitations and safeguards; and

iii. any relevant contractual, technical, or organisational safeguards put in place to supplement the safeguards under the Processor Policy, including measures applied during transmission and to the processing of the personal information in the Non-Adequate Location.

Laws and practices of third country of destination

3.5 As regards the impact of the laws and practices of the Non-Adequate Location on compliance with the Processor Policy, different factors may be considered as part of an overall assessment. Such factors may include, for example, the Data Recipient's practical experience with prior instances of disclosure requests from public authorities, or the absence of such requests. This may be drawn from internal records or other documentation, provided that this information can be lawfully shared with third parties.

3.6 Where this practical experience is relied upon to conclude that the Data Recipient will not be prevented from complying with the requirements of the Processor Policy, such conclusion needs to be supported with relevant, objective evidence, and it is for the Privacy Team, the

Data Transferor and Data Recipient to consider carefully whether this evidence carries sufficient weight, in terms of their reliability and representativeness, to support the conclusion.

3.7 In particular, the Privacy Team, the Data Transferor and Data Recipient have to take into account whether upon reasonable due diligence, the practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the laws in practice, such as case law and reports by independent oversight bodies.

Findings of Transfer Impact Assessments

3.8 The Privacy Team shall make available to other relevant Group Members the findings of the Transfer Impact Assessment, so that they, or where applicable the Privacy Team, can (if required) apply any identified additional safeguards determined to be necessary in respect of any identical or similar subsequent transfers they make.

3.9 Where the Transfer Impact Assessment concludes that it is not possible to implement additional safeguards to ensure the Data Recipient's processing in the Non-Adequate Location will be compatible with the requirements of the Processor Policy, then the Privacy Team shall inform the Data Transferor (and other relevant Group Members) and shall instruct the Data Transferor to not proceed with any such transfer of personal information where effective supplementary measures could not be put in place, and in such circumstances, the transfers at stake will be suspended or ended.

Information and cooperation

3.10 If the Data Recipient is a Group Member, the Data Recipient must use its best efforts to provide the Privacy Team and the Data Transferor with relevant information and cooperate with the Privacy Team and the Data Transferor to ensure compliance with the requirements of the Processor Policy throughout the duration of the transfer and subsequent processing.

3.11 If the Data Recipient is not a Group Member (i.e., if it is a third-party data recipient), the Privacy Team and the Data Transferor must exercise appropriate diligence to ensure that the Data Recipient has used such best efforts and will continue to provide such cooperation, including where appropriate by seeking contractual assurances from the Data Recipient.

3.12 The Privacy Team and the Data Transferor will coordinate with the Data Recipient to document the Transfer Impact Assessment as well as documenting any supplementary measures selected and implemented in relation to such transfers and, where requested, to make these or a relevant summary (where applicable) available to the Controller and the competent supervisory authority on request.

4. Transfer Risk Notifications

4.1 If the Data Recipient is a Group Member, the Data Recipient or, where applicable, individual personnel supporting the Data Recipient must notify the Privacy Team and the Data Transferor promptly if, at any time during which it receives or processes personal information from the Data Transferor, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements of the Processor Policy, including following a change in the laws of the Non-Adequate Location where it receives or processes personal information or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements of the Processor Policy (a "**Transfer Risk Notification**").

4.2 When located in an EU member state, the Data Transferor will take reasonable steps to monitor, on an ongoing basis, and where appropriate in collaboration with Data Recipients, developments in the Non-Adequate Country to which the Data Exporter has transferred personal information that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers and in particular in relation to developments that may affect the outcome of the Transfer Impact Assessment.

4.3 If the Data Recipient is not a Group Member (i.e., if it is a third-party data recipient), the Privacy Team and the Data Transferor must exercise appropriate diligence to ensure that the Data Recipient will provide any such Transfer Risk Notification to the Privacy Team and the Data Transferor, including where appropriate by seeking documented assurances from the Data Recipient.

4.4 Following receipt of a Transfer Risk Notification from the Data Recipient, or if the Privacy Team or the Data Transferor otherwise have reason to believe that the Data Recipient's processing is (or is at risk of becoming) incompatible with the obligations under the Processor Policy, the Privacy Team and the Data Transferor shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality)

to be adopted by the Data Transferor and Data Recipient to address the situation, if appropriate in consultation with the Controller.

4.5 The Privacy Team shall instruct the Data Transferor to suspend the transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if the Data Transferor is instructed by the Controller or the competent supervisory authority to do so.

4.6 In this case, the Data Transferor shall be entitled to terminate its transfers of personal information to the Data Recipient, insofar as it concerns the processing of personal information under the Processor Policy (in which event, the Data Recipient must be required to return or destroy the personal information it received, as instructed by the Data Transferor).

4.7 If the Data Transferor transfers personal information to two or more Data Recipients, the Data Transferor may exercise this right to terminate only with respect to the relevant Data Recipient.