

HPE Binding Corporate Rules for Processor - FAQs for HPE Customers

1. Are HPE BCR-P available for all HPE services and to all Customers?

HPE BCR-P are available from 1 May 2019 to all Customers. HPE BCR-P apply to HPE services listed on the [HPE BCR website](#). We have taken steps in our intragroup agreement (which forms part of the BCRs) to ensure that the BCR-P are made binding on all participating members of the HPE Group and their employees.

2. How can you rely on HPE's BCR-P for an HPE service?

If you are concluding and/or renewing a Services Agreement for HPE services after 1 May 2019, you will need to ensure that the BCR-P are incorporated by reference into the agreement with the relevant HPE Company. Updated Services Agreements for the HPE services covered by BCR-P are available at our [Privacy Terms and Sub-processor Transparency](#) website. In summary, you must agree that the HPE entity can receive and transfer EU Customer Personal Data in a Relevant Country in accordance with the HPE BCR-P.

You must also inform any relevant EU Data Subjects that:

- if the transfer of their Personal data involves Special Category Data, this could include transfers to a Relevant Country; and
- Processors may exist in Relevant Countries and that you are relying on the HPE BCR-P as required by applicable data protection laws, making available a link to HPE's [BCR Rights Notice](#) on request.

Upon your request, we will provide you with a full copy the HPE BCR-P Intercompany Agreement. You do not need to make any additional notifications to any EU or UK supervisory authorities before you can rely on our BCR-P.

If you have an existing Services Agreement for HPE services, there is no need for you to take any action as the Services Agreement includes EU Standard Contractual Clauses on the basis of which HPE entities receive and transfer EU Customer Personal Data in a Relevant Country. However, if you wish to change to HPE BCR-P before your Services Agreement's term expires or is terminated, please contact your HPE primary contact and/or HPE Privacy Office by clicking [here](#).

3. What are our commitments to you under our BCR-P?

Privacy Principles

We commit to provide reasonable help and assistance to enable you to meet the applicable European data protection principles.

This includes:

(i) Transparency, fairness and lawfulness

Providing reasonable help and assistance to comply with the transparency, fairness and lawfulness principle (e.g. being transparent about our sub-processor activities so you can properly inform the data subjects).



(ii) Purpose Limitation

Ensuring that there is a Services Agreement in place with you which covers the processing of EU Customer personal data and which includes security and confidentiality provisions and the mandatory privacy terms provided by Article 28 GDPR. The BCR-P contain provisions which are substantially similar and are binding on all HPE companies.

We will respect your written instructions regarding the data processing and the security and confidentiality measures provided in the Services Agreement and will promptly tell you (unless prohibited by law) if we are unable to comply for any reason.

We will comply with all applicable HPE Privacy Policies and other applicable policies, standards and procedures comprised in the BCR-P; and all applicable local data protection and privacy laws. If local law requires a higher standard of data protection than the BCR-P, the local law takes precedence over the BCR-P.

(iii) Data Quality

Updating, correcting or deleting EU Customer Personal Data in accordance with your instructions to the extent that you are unable to access the relevant data yourself and where applicable, given the nature of the processing, inform any other HPE Companies or third parties to whom EU Customer Personal Data has been disclosed that this has been done.

At your request, we will, to the extent reasonably possible and within a reasonable period of time, put in place measures to delete or anonymize the EU Customer Personal Data when you determine that identification of EU Data Subjects is no longer necessary and where applicable, given the nature of the processing inform any other HPE Companies or third parties to whom EU Customer Personal Data has been disclosed that this has been done.

(iv) Security

Implementing appropriate technical and organisational measures to protect EU Customer Personal Data against Personal Data Breaches. We will also take into account any applicable data protection laws which apply to you and any measures specified in the Services Agreement.

If there is a Personal Data Breach, we will follow HPE's Security Incident Management Process In the case of EU Customer Personal Data, this includes requirements for HPE Companies to:

- keep records of Personal Data Breaches; and
- notify you without undue delay after becoming aware of the Personal Data Breach, all in a manner which meets applicable data protection laws.

We shall also provide reasonable assistance to you to enable you to meet your obligations with respect to security, privacy by design and by default, Personal Data Breaches and data protection impact assessments (as set out in applicable data protection law), taking into account the nature of the processing and the information available to the relevant HPE Company.



Hewlett Packard Enterprise

(v) **Assisting you with Data Subject Rights**

Promptly forwarding any communication or access request received directly from any EU Data Subject to you, without responding to it unless requested by you.

We will also provide copies of any EU Customer Personal Data which you need to be able to respond to a communication or access request to the extent you are unable to access the relevant data yourself.

Also, at your request, we will put in place appropriate and reasonable technical and organisational measures, insofar as possible, to assist you in complying with any legal duty you have to respect the rights of data subjects under applicable data protection law.

(vi) **Sub processing**

Sub processing within the HPE Group

Not transferring or permitting another HPE Company to have access to or process EU Customer Personal Data unless that company is a signatory to the BCR-P and it has your specific or general authorization.

Sub processing outside the HPE Group

Not transferring EU Customer Personal Data to a third party sub processor unless we have your consent (which can be provided in a number of different ways). We will also ensure that we have a written agreement in place with the sub processor which includes obligations substantially similar to the relevant obligations in the Services Agreement, certain requirements of the BCR-P and ensures the adequate protection of any data transferred internationally in accordance with applicable data protection laws.

Appointing Replacement Sub-Processors

Notifying you of any new or replacement sub processors in such a timely fashion in so that you may object to this change.

Responsibility for Acts & Omissions of Sub-Processors

Remaining responsible and liable for the acts and omissions of any sub processors that result in a breach of the BCR-P.

(vii) **Accountability and Audits**

Providing you with all information necessary (taking into account the nature of the processing and the information available to us) to demonstrate compliance with your obligations under applicable data protection laws and allow for and contribute to audits.

Each HPE Company must implement appropriate data privacy and security training developed by the Privacy Office and the HPE Cyber Security team from time to time.

(viii) **Deletion or Destruction of Personal Data on Termination**



Hewlett Packard Enterprise

Complying with your instructions to return, delete or destroy all copies of EU Personal Data on termination of the Processing of EU Customer Personal Data or on termination of the Services Agreement, and certifying that this has been done.

If we are required by law to retain any EU Customer Personal Data, we will keep the data confidential and put in place appropriate security to protect the data.

(ix) **Data Retention**

Retaining EU Customer Personal Data for the term of your Services Agreement unless otherwise instructed by you or by other written instruction.

Cooperation

All HPE Companies must cooperate with you, any EU Data Subjects and the appropriate EU Supervisory Authority to verify our compliance with the BCR-P, answer any questions or respond to any complaints relating to the processing of Personal Data in accordance with the BCR-P.

Updates to the BCRs

HPE may update, amend or modify the BCR-P from time to time (including the list of any approved third party sub-processors) and will notify all HPE Companies of such changes. You will be notified of any such changes where you have a Services Agreement with us and where a change would affect a processing condition, such information will be provided in a timely fashion to ensure that you have the possibility to object to the change.

National Legislation prevents compliance

We will promptly update you if we have reasons to believe that any existing or future applicable legislation prevents us from fulfilling any instructions received from you.

We will also notify you of any legally binding requests for disclosure of EU Customer Personal Data by a law enforcement body (unless prohibited from doing so).

4. Can you enforce the BCR-P?

Yes, the BCP-P are made binding to you by means of a third party rights clause which shall include the right to:

- Lodge a complaint before the applicable supervisory authority in the jurisdiction in which you are established where you have the right to do so under applicable data protection law;
- Bring a claim for damages against the HPE Company which has signed the Service Agreement with you or against Hewlett Packard the Hague B.V (for breaches caused by other HPE Companies or third party sub-processors).

We have also included measures to ensure that EU Data Subjects can enforce their rights as third party beneficiaries directly against the HPE Group in certain circumstances and receive compensation for any damage suffered, as required by applicable law including where you have factually disappeared, ceased to exist or became insolvent.



Hewlett Packard Enterprise

Any complaints from an EU Data Subject shall be communicated to you without undue delay and we will not respond to such complaints unless otherwise agreed with you or where you have factually disappeared, ceased to exist or became insolvent. Any complaints we do handle shall be dealt with without undue delay and in any event within a month (except in exceptional circumstances). For more information, see our [BCR Rights Notice](#).

HPE Privacy Office Organization

The HPE Privacy Office oversees our privacy compliance program. The HPE Privacy Office is responsible for ensuring compliance with HPE Privacy Policies, including the BCR-P. The Privacy Office is authorised to investigate any failure by an HPE Company to comply with the BCR and will consult with the relevant supervisory authority in order to decide on the appropriate action, if necessary or appropriate.

Each HPE Company has to comply with any decision issued by the HPE Privacy Office if they are found to be non-compliant with the BCR-P.

Glossary

EU Customer Personal Data	Means any personal data in relation to which (i) the Customer is the controller or (ii) the Customer is a processor on behalf of a controller which has authorised the appointment of any HPE Company as sub-processor, and which is processed by an HPE Company in order to deliver an HPE Service and to which GDPR or the laws of EEA, Switzerland or the UK (once the UK has ceased to be a member state of the EU) applies.
EU Data Subjects	Means any individual to whom EU Personal Data applies.
HPE	Means Hewlett Packard Enterprise Company, which has its headquarters in the US.
HPE Company	Means a member of the HPE Group which has signed the Intracompany Agreement which binds each entity to comply with the BCR-P. For a list of signatory companies, please check HPE BCR website and/or contact the Privacy Office by sending email to hpeprivacy@hpe.com .
HPE Group	Means HPE and all its majority owned and controller subsidiaries irrespective of jurisdiction of incorporation or operation.
Personal Data Breaches	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to Customer Personal Data.
Relevant Country	Means a third country outside of the EEA, Switzerland and the UK (once the UK has ceased to be a member state of the EU) which has not been given an adequacy finding pursuant to the GDPR or other applicable data protection laws.



**Hewlett Packard
Enterprise**

Services Agreement	Means any written contract between an HPE Company and a Customer for HPE Services, which applies the BCR-P to the Processing and transfer of Customer Personal Data in whole or in part connection with the provision of the relevant HPE Services.
Special Category Data	Means personal data revealing racial or ethnic origins; political opinions, religious or philosophical beliefs or trade union membership and genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or a natural person's sex life or sexual orientation.