HP Inc.
Binding Corporate Rules

October 2018
Public Version

Table of contents

1 Introduction 3

2 Summary of the BCRs 4

3 Scope of the BCRs 5

3.1 Lawfulness & Fairness 5

3.2 Transparency, Notice & Choice of Data Use 6

3.3 Purpose Limitation 6

3.4 Data Quality 6

3.5 Data Security & Data Breach Notification 7

3.6 Automated Decision Making 8

3.7 Onward Transfer 8

4 HP's Commitments 10

4.1 Governance 10

4.2 Training 10

4.3 Compliance Assurance 10

4.4 Cooperation 10

4.5 Honoring Data Subject Rights 11

5 Submitting a Complaint and Enforcing the BCRs 12

5.1 HP's Complaint Handling Process 12

5.2 Complaint Escalation 12

5.3 Third-Party Enforcement Rights 13

6 Updates to HP's BCRs 14

7 Conflicts of Law 15

Glossary 16

1 Introduction

HP recognizes the importance of privacy as a basic human right. We have developed a data protection program to ensure respect for privacy throughout all aspects of our operations. We comply with privacy and data protection laws around the world and apply the highest possible standards in a consistent way globally in order to provide consistent protections to our customers in jurisdictions that do not yet have data protection laws.

HP's commitment to privacy and data protection was recognized in 2011 when HP's Binding Corporate Rules for Data Controller were approved by European regulators and permit HP to transfer the Personal Data of HP employees and consumers outside of the European Union ("EU"). In 2018, European regulators again recognized HP's commitment to privacy and data protection by approving a set of Binding Corporate Rules for Data Processor that apply when HP is processing data on behalf of commercial customers.

HP's Binding Corporate Rules for Data Controller and Data Processor (collectively "BCRs") set the minimum standards for protection of Personal Data by the HP Companies that are bound by the BCRs.

Please see the Glossary at the end of this Public Summary for definitions of capitalized terms. References to "process or processing" means to include any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction.

2 Summary of the BCRs

The BCRs consist of HP's corporate policies, privacy standards and specifications, commitments to training and assurance, and Data Subject enforcement rights. HP's BCRs apply in the following situations:

- *HP as Data Controller:* HP's BCRs for Data Controller apply when HP processes Personal Data from consumers, vendors, business partners, business contacts, current and former HP employees, and job applicants.

- *HP as a Data Processor:* HP's BCRs for Data Processor apply when HP processes Personal Data on behalf of a Data Controller (either directly or indirectly via a third-party Data Processor). This could include the Personal Data of the Data Controller's employees or customers.

The BCRs are made binding through two Intercompany Agreements on the Processing and Transfer of Personal Data ("Intercompany Agreement(s)"). An updated list of all HP Companies that have executed the Intercompany Agreements and are consequently bound by the BCRs can be found at www.hp.com/privacy.

Furthermore, all HP employees are bound by the BCRs through HP's internal standards of business conduct and HP policies, standards and specifications applicable to the collection and processing of Personal Data.

Where local law requires a higher standard of data protection than HP's BCRs, local law takes precedence over the BCRs.

If you are an HP employee, please visit the HP Privacy and Data Protection Office's intranet site for additional details regarding HP's processing of employee data in accordance with its BCRs.

3 Scope of the BCRs

HP's BCRs are based on HP's accountability-based privacy and data protection program which centers on the fundamental principles set forth in this section. Where HP's obligations differ depending on its role as a Data Controller versus a Data Processor, such distinctions are noted.

3.1 Lawfulness & Fairness

HP only processes Personal Data fairly and in accordance with law. HP is careful to take account of a Data Subject's reasonable expectations whenever it processes their Personal Data.

Data Controller

As a Data Controller, HP primarily processes Personal Data based on the following legal bases:

- *Consent* - Data Subjects have unambiguously given consent.
- *Contract Performance* - Processing is necessary for the performance of a contract to which a Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- *Required by Law* - Processing is necessary for compliance with a legal obligation.
- *Legitimate Interests* - Processing is necessary for the purposes of the legitimate interests pursued by HP, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject.

Moreover, HP recognizes that additional care is required to justify the processing of any Sensitive Personal Data and, therefore, HP is prohibited from processing Sensitive Personal Data unless one of the following apply:

- *Consent* - Data Subjects have given explicit consent to the processing of Sensitive Personal Data.
- *Legal Obligations* - Processing is necessary for the purposes of carrying out HP obligations and rights in the field of employment and social security and social protection law in so far as it is authorized by national law providing for adequate safeguards.
- *Vital Interests* - Processing is necessary to protect the vital interests of the Data Subject or of another person.
- *Publicly Available* - Processing relates to Sensitive Personal Data which are manifestly made public by the Data Subject.
- *Legal Claims* - The processing of Sensitive Personal Data is necessary for the establishment, exercise or defense of legal claims.
- *Public Interest* - The processing is necessary for reasons of substantial public interest based on local law.

Data Processor

When HP processes data on behalf of a Data Controller, it is the Data Controller that is responsible for ensuring that any such processing is based on the appropriate legal grounds. HP will only process Personal Data in accordance with the instructions provided by the Data Controller.

3.2 Transparency, Notice & Choice of Data Use

HP operates transparently and provides clear notice to Data Subjects about the identity of the Data Controller, purposes of processing, categories of Personal Data collected, recipients of the Personal Data and other information as required by law. HP also provides Data Subjects with choices about what information can be collected and how that information can be used.

3.3 Purpose Limitation

HP abides by the principal of purpose limitation and only uses Personal Data for the purposes described at the time of collection or strictly in accordance with instructions from the Data Controller.

Data Controller

When acting as a Data Controller, HP only uses Personal Data for the purposes described at the time of collection or for additional compatible purposes in accordance with law. HP has implemented "Privacy by Design" which requires that all HP systems, services, applications and products be designed and implemented with privacy in mind. As part of the Privacy by Design process, HP carefully reviews the purposes for which Personal Data is to be collected to ensure that our data collection supports reasonable business requirements and is proportionate to our needs. HP will not use Personal Data for purposes that are incompatible with the notices provided to or the choices made by Data Subjects.

Data Processor

HP processes Personal Data on behalf the Data Controller only for the purposes of delivering our services and in compliance with:

- the terms of the relevant agreement between HP and the Data Controller, including, those relating to the security, confidentiality and any processing instructions of the Data Controller;
- any other documented processing instructions between the Data Controller and HP;
- all applicable HP privacy policies;
- HP's BCRs; and
- all local data protection and privacy laws applicable to HP.

3.4 Data Quality

HP respects the principle of data quality and takes steps to ensure that the Personal Data it processes is up-to-date and accurate.

Data Controller

When acting as a Data Controller, HP takes reasonable steps to ensure that Personal Data is accurate, complete and current. HP also only keeps Personal Data in a form which permits the identification of Data Subjects for only as long as is necessary for the purposes for which it is collected. Personal Data that it is no longer necessary or that HP is no longer legally required to maintain is securely deleted or destroyed.

Data Processor

When processing Personal Data on behalf of a Data Controller, HP will take steps to update, correct or delete Personal Data in accordance with the Data Controller's direction. HP retains Personal Data only

to the extent it is necessary to provide the Data Controller with our services, unless otherwise instructed by the Data Controller or required by law. Upon instruction from the Data Controller, HP complies by either deleting, destroying or facilitating the return of the Personal Data to the Data Controller depending on the nature of the instruction.

3.5 Data Security & Data Breach Notification

Protection of Personal Data is one of HP's greatest responsibilities. Accordingly, HP has implemented a robust set of information security controls including policies, practices, procedures and organizational structures to protect the confidentiality, integrity and availability of Personal Data. In general, HP's security controls are intended to protect against physical, organizational and logical threats and include measures to address the following:

- Security Policy
- Information Security Organization
- Asset Management
- Access Control
- Personnel Training
- Third Parties and Subcontractors
- Systems Security
- Physical and Environmental Security
- Operations Management
- Cryptography
- Information Security Incident Management
- Business Continuity Management

To learn more about HP's Security Measures, click here.

Data Controller

When acting as a Data Controller, HP implements appropriate technical and organizational measures to protect against unauthorized or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. These measures are appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of Personal Data and having regard to the nature of the Personal Data which is to be protected. In addition, HP takes into account the state of the art and the costs of implementation of such technical and organizational measures. HP also extends its security requirements to third-party service providers that process Personal Data on behalf of HP.

In the event of an actual or suspected security breach involving Personal Data, HP follows the appropriate incident management and breach notification processes. These processes include requirements for HP to:

- Keep records of all Personal Data incidents;
- Notify Data Subjects of incidents affecting Personal Data where the breach is likely to result in a high risk to the Data Subject; and
- Notify incidents affecting Personal Data to the Supervisory Authority where required.

Data Processor

With regard to HP's activities as a Data Processor, HP complies with its legal obligations by implementing security measures that are suitable to the nature of the Personal Data and processing activities undertaken on behalf of the Data Controller, along with the potential harm that might come to the Data Subject. Furthermore, HP implements any additional security measures required by the Data Controller and set forth in the agreement governing the provision of our services. To the extent that any

HP security measures exceed the legal minimums or the requirements set by the Data Controller, HP always implements the more protective measures.

If HP becomes aware of any actual or suspected security incident involving the Data Controller's Personal Data, HP will notify the Data Controller without undue delay. HP will also cooperate with the Data Controller to remedy the security incident and provide information necessary for the Data Controller to satisfy its breach notification obligations.

3.6 Automated Decision Making

Data Subjects have the right not to be subject to a decision which is based solely on automated processing to evaluate personal aspects of the Data Subject and: 1) results in legal effects concerning the Data Subject; or 2) otherwise significantly affects the Data Subject. The only circumstances in which HP can make automated processing decisions is if the decision is based on one of the following:

- *Consent* – The Data Subject has provided their explicit consent.
- *Contract Performance* – The decision is taken in the course of entering into or the performance of a contract between HP and the Data Subject, provided the request for the entering into or the performance of the contact was made by the Data Subject.
- *Authorized by Law* – Local law permits such decisions and includes measures to safeguard the Data Subject's legitimate interests.

3.7 Onward Transfer

In all cases, HP will only engage a Data Processor (whether another HP Company or a third party, including sub-processors) to process Personal Data if it is permitted to do so by applicable HP policy and the Data Processor is able to provide sufficient guarantees of compliance with applicable privacy and data protection laws.

Data Controller

Where a HP company is acting as a Data Controller, before transferring the data to any other HP entity for processing, the HP entity acting as a Data Processor must agree to comply with the obligations set forth in the applicable Intercompany Agreement. The obligations contained in the Intercompany Agreement serve as the binding written agreement that satisfies Article 29 of the EU General Data Protection Regulation. In other words, within the HP group of companies, Personal Data can only be transferred between HP companies that are parties to the applicable Intercompany Agreement.

When transferring Personal Data outside of the HP group to a third-party Data Controller, HP will ensure that the Personal Data is adequately protected by complying with applicable privacy and data protection laws.

With regard to transfers to third-party Data Processors, HP only transfers Personal Data to third-party Data Processors located in Adequate Third Countries or in accordance with the following legal mechanisms:

- EU Standard Contractual Clauses;
- EU – U.S. Privacy Shield;
- EU – Swiss Privacy Shield; or

- Binding Corporate Rules.

In all cases of onward transfer to third parties, HP shall ensure that it enters into a written agreement with the third party which contains provisions no less protective than those set out in HP's BCRs.

Data Processor

When acting as a Data Processor, an HP company will not transfer to or permit another HP company to act as a sub-processor or to have access to or process Personal Data unless: 1) that company is a signatory to the appropriate Intercompany Agreement; and 2) HP has provided the proper notification and obtained the prior written consent of HP's customer which may be either a Data Controller or a Data Processor.

Similarly, when HP transfers Personal Data to a third-party sub-processor, it shall only do so if it has provided the appropriate notice and obtained the necessary authorizations from its commercial customers (acting as either Data Controllers or Data Processors). In addition, HP will only transfer data to third-party sub-processors in accordance with the legal mechanisms set forth above and with a written agreement in place that contains terms no less protective than those set out in HP's contract with its customer.

HP is responsible for the acts and omissions of any HP or third-party sub-processors and remains fully liable for the acts and omissions of the sub-processors giving rise to a breach of HP's BCRs as if they were HP's own acts or omissions.

4 HP's Commitments

Central to the BCRs are HP's commitments to maintain a robust corporate framework for privacy and data protection. These commitments include:

4.1 Governance

HP's Privacy and Data Protection Office is led by the Chief Privacy and Data Protection Officer who reports into the Ethics and Compliance Office in HP's Global Legal Affairs. The Chief Privacy and Data Protection Officer regularly reports to HP's Board of Directors through the Audit Committee. The Privacy and Data Protection Office is chartered to ensure compliance with applicable privacy and data protection laws and is responsible for overseeing compliance with HP's BCRs.

4.2 Training

Employee training is critical for ensuring the protection of Personal Data. In addition to general privacy training required for all employees, HP has implemented role-based training programs that cover, among other things: risks to data; security measures to prevent dangerous events; data protection principles according to the law and HP policies; and employee responsibilities. HP also has specialized trainings to address the compliance obligations under its BCRs.

The HP Privacy and Data Protection Office develops and refreshes trainings on an ongoing basis using a variety of resources and materials. Depending on business needs, risk assessment outcomes, assurance processes and other factors, the HP Privacy and Data Protection Office may develop additional role-based and/or mandatory trainings.

4.3 Compliance Assurance

The HP Privacy and Data Protection Office is responsible for the implementation of HP's Privacy Assurance program. This program is designed to assess internal compliance with HP's internal privacy policies, standards, specifications and BCRs. Through this program, HP identifies potential compliance gaps and tracks and mitigates risks. The program covers all business units and functions that collect, use, access, or store Personal Data. The results of any internal assessment shall be communicated to the appropriate stakeholders.

HP's BCRs are subject to an annual audit during which the Privacy and Data Protection Office will ensure that Personal Data is being protected and HP companies are acting in compliance with their obligations under the BCRs.

HP also monitors compliance through third-party certifications, dispute-resolution mechanisms and robust monitoring of Data Subject complaints and feedback.

4.4 Cooperation

HP shall cooperate with any Data Subjects, commercial customers (acting as Data Controllers or Data Processors) and Competent Supervisory Authorities to verify HP's compliance with its BCRs, answer any questions or respond to any complaints relating to the processing of Personal Data in accordance with its BCRs.

4.5 Honoring Data Subject Rights

Data Controller

HP will honor Data Subject rights under applicable data protection laws and will seek to accommodate the rights in a clear and transparent manner without undue delay, unless applicable law permits or requires HP to deny the rights. This includes rights for Data Subjects to:

- Obtain information about what Personal Data HP holds and how such data is processed;
- Rectify any Personal Data relating to them that is inaccurate;
- Erase or restrict processing of their Personal Data;
- Request their Personal Data to be transferred to a third party;
- Object to direct marketing (including profiling linked to direct marketing);
- Object to certain types of processing in special situations; and
- Not be subject to entirely automated decisions (including profiling) which produce legal effects or significantly affect individuals.

These rights may be limited in some situations under applicable law.

Data Processor

HP will notify its commercial customers (acting as Data Controllers or Processors) if they receive a Data Subject request relating to the Personal Data that HP is processing on behalf of its commercial customer. HP will cooperate with its commercial customers in responding to requests by Data Subjects to exercise their rights.

5 Submitting a Complaint and Enforcing the BCRs

HP recognizes that where Personal Data has not been processed in accordance with its BCRs, Data Subjects may also have the right to seek redress by filing a complaint with HP or filing a complaint or seeking redress from a Relevant Supervisory Authority or Court. The following sets forth how a Data Subject can file a complaint or seek to enforce HP's BCRs.

5.1 HP's Complaint Handling Process

Data Controller

HP has implemented a complaint management process and applies consistent incident management procedures from identification through to resolution. Complaints relating to HP's BCRs can be submitted through the following mechanisms:

- *Online* - Complaints can be submitted via the "Contact HP Privacy Office" form.
- *Postal Mail* - Complaints can be sent to HP via mail service at the addresses listed in HP's Privacy Statement or Personal Data Rights Notice.
- *Telephone* - Complaints can be reported via telephone using the local number provided in the Personal Data Rights Notice.

Upon receipt, the HP Privacy and Data Protection Office will review the submission and take action to honor requests, investigate complaints and/or respond to inquiries. HP will acknowledge receipt of a complaint within ten U.S. business days and will respond to all submissions in accordance with legal requirements.

Data Processor

Where HP is processing Personal Data on behalf of a commercial customer, HP strongly encourages Data Subjects to submit their request or complaint directly to the Data Controller, who will instruct HP on necessary actions. If HP receives a request or complaint directly from the Data Subject, it shall promptly notify its commercial customer and comply with any subsequent requests by the Data Controller in support of its efforts to respond to the request or complaint. If HP's commercial customer is a Data Processor, HP will inform the commercial customer and, if directed, also inform the Data Controller.

If the Data Controller is no longer in existence, then HP will respond directly to the Data Subject.

5.2 Complaint Escalation

If the Data Subject is not satisfied with HP's response, they have the right to seek redress by: 1) filing a complaint with a Supervisory Authority; and 2) seeking a judicial remedy in court. It is important to note, however, that at any time, individuals may seek redress with the Relevant Supervisory Authority or Court without first filing a complaint with HP or exhausting the HP Complaint Handling Process. HP is committed to working with the Relevant Supervisory Authorities or Court to resolve any complaints filed alleging non-compliance with HP's BCRs.

5.3 Third-Party Enforcement Rights

HP recognizes that data protection laws contain remedies for Data Subjects that give them the right to lodge complaints, obtain redress and, where appropriate, seek compensation where HP or its third-party sub-processors fail to process Personal Data in accordance with HP's BCRs. Data Controllers and Data Subjects are entitled to full access of the sections of HP's BCRs as they apply to third-party beneficiary rights, namely the following:

- Part IV, Section 1 of the Intercompany Agreement on the Processing and Transfer Personal Data
- Sections 4 and 5 of the Intercompany Agreement on the Processing and Transfer of HP Customer-Owned Personal Data within the HP Group

Requests for access can be submitted via Contact HP Privacy Office.

Data Controller

In situations where HP acts as a Data Controller, Data Subjects can enforce their rights as third-party beneficiaries in relation to a breach by either the HP company acting as the Data Importer or the HP company acting as the Data Exporter. In such cases, the HP company that acted as the Data Exporter shall accept liability for such breach as if it had arisen from its own act or omission.

Data Processor

If HP, when acting as a Data Processor, processes Personal Data in breach of its BCRs, HP's commercial customer (or, if the commercial customer is a Data Processor, the Data Controller on whose behalf the commercial customer processes the Personal Data) has the right as a third-party beneficiary to enforce the BCRs and lodge a complaint or bring a claim for compensation for damages against HP with the applicable Supervisory Authorities or courts. Where the breach is caused by the HP company acting as the Data Importer or a third-party sub-processor of an HP company, commercial customers have the right to enforce the BCRs against the HP company acting as the Data Exporter or HP's pre-designated EU entity.

In addition, where the Data Controller ceases to exist, Data Subjects also have the right as third-party beneficiaries to HP's BCRs to file complaints or to bring a claim for compensation for damages against HP's pre-designated EU entity, which shall accept liability for such breach as if it had arisen from its own act or omission.

To request additional information regarding the rights of HP customers or information regarding HP's pre-designated EU entity, against which complaints may be lodged, please submit your request via Contact HP Privacy Office.

In the event that the Data Subject is not able to bring a claim against the Data Controller, or the laws of the Data Subject's place of residence or establishment do not allow the Data Subject to bring such a claim, the Data Subject may exercise his or her rights to seek remedies or lodge a complaint in:

- the jurisdiction of the HP company acting as Data Exporter from which the data transfer originated; or
- the jurisdiction of the European headquarters of the HP Group; or
- the EU Member State in which the HP Group's designated entity for data protection responsibilities is established, namely the Netherlands.

6 Updates to HP's BCRs

HP's BCRs may be updated, amended or modified by HP from time-to-time. Any such updates shall be notified to HP companies which shall have an opportunity to object to any such changes.

Data Controller

HP will ensure that significant amendments are communicated to Data Subjects via email, posting on an internal website, or other such method. HP will also provide notice of any substantial changes to the Commission nationale de l'informatique et des libertés ("CNIL") on an annual basis. Where a modification would affect the level of the protection offered by the BCRs, such changes shall be promptly communicated to the CNIL.

Data Processor

Where amendments will affect data processing conditions, HP will notify its commercial customers in a timely fashion such that the commercial customer has the possibility to object or to terminate the agreement covering the provision of our services before the amendment is made or the termination becomes effective.

HP will provide notice of significant changes to the CNIL on an annual basis.

7 Conflicts of Law

Data Controller

Where local laws may prevent HP from complying with its obligations under the BCRs or have a substantial impact on the guarantees provided by the BCRs, HP will involve the Competent Supervisory Authority. Where HP considers that the matter would have a substantial adverse effect on the guarantees provided by the BCRs, it will report the matter to the Competent Supervisory Authority as required to settle the case in collaboration with appropriate government authorities. This includes any legally-binding requests for disclosure of the Personal Data of an EU Data Subject by a law enforcement or state security body.

If HP is prohibited by law or a law enforcement authority from disclosing such matters, HP will use commercially reasonable efforts to obtain a right to waive such prohibition and be in a position to provide as much information as possible to the CNIL and any other Competent Supervisory Authority and if requested by the Competent Supervisory Authority, provide information to demonstrate what actions it has taken under this section (unless this would be prohibited by secrecy requirements).

If, despite having used commercially reasonable efforts, the HP is unable to lawfully notify the CNIL and any other Competent Supervisory Authority it shall, on an annual basis, publish general information on the requests received by HP.

HP shall ensure that any disclosures made to law enforcement authorities or state security bodies in response to a request shall be made in accordance with applicable data protection laws.

Data Processor

When HP is acting as a Data Processor, upon receipt of a legally binding request for disclosure of Personal Data by a law enforcement authority or a state security body, HP will notify the commercial customer unless prohibited from doing so, for example, as the result of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

Where the request relates to Personal Data, and where HP is not prohibited from doing so, on a case-by-case basis, HP will assess whether to notify the Competent Supervisory Authority and provide details of the requestor, the Personal Data requested and the legal basis for the disclosure by HP.

Where HP is prohibited disclosing the request, it shall use commercially reasonable efforts to obtain a right to waive such prohibition and be in a position to provide as much information as possible to its commercial customer and/or the Competent Supervisory Authority.

If, despite having used commercially reasonable efforts, HP is unable to lawfully provide such notifications, on an annual basis, HP will publish general information on the requests received by HP for Personal Data.

Glossary

Adequate Third Countries - Means any EU, EEA country or other third country that is determined as offering adequate protection for Personal Data pursuant to applicable data protection law. As of May 2018, the following countries are subject to a finding of adequacy by the European Commission – Andorra, Argentina, Canada, Isle of Man, Jersey, Faeroe Islands, Guernsey, New Zealand, State of Israel, Switzerland, Uruguay and, US companies certified to the EU-US Privacy Shield.

Data Controller - Means an entity (whether a natural or legal person, public authority, agency or other body) which alone, jointly or in common with others determines the purposes and means in which any item of Personal Data is processed.

Data Exporter – Means the HP BCR Company established in the EU or EEA who exports Personal Data to a Data Importer located in a third country (i.e., outside of the EU, EEA, or Adequate Third Country).

Data Importer - Means the HP BCR Company established in a third country (i.e., outside of the EU, EEA, or Adequate Third Country) who agrees to receive Personal Data from another HP BCR Company located in the EU or EEA.

Data Processor - Means an entity (whether a natural or legal person, public authority, agency or any other body) which processes Personal Data on behalf and upon instructions of the Data Controller.

Data Subject - Means an identified or identifiable individual natural person to whom Personal Data relates.

European Economic Area (EEA)- Means the zone of economic cooperation known as the European Economic Area and those countries which are participants in such zone, collectively.

European Union (EU)- Means the political grouping known as the European Union and those countries which are members of such political union, collectively.

Personal Data - Means any information relating to an identified or identifiable natural person; an identifiable 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, online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, including Sensitive Personal Data and any other data deemed to be personal data under applicable data protection law.

Sensitive Personal Data - Means Personal Data revealing racial or ethnic origins; political opinions or affiliations; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purposes of uniquely identifying a natural person, health or sex life; and criminal convictions, offences, or proceedings.

Supervisory Authority - Means a body with regulatory powers with respect to the protection of Personal Data.

Competent Supervisory Authority – Means:

(i) the CNIL; or
(ii) any other Supervisory Authority which is "concerned" by the processing of Personal Data because:
  (a) an HP BCR Company is established in the country or territory in which that Supervisory Authority is established;
  (b) Data Subjects living in the country or territory of that Supervisory Authority are likely to be affected by an HP BCR Company's processing of Personal Data, or
  (c) it has received a complaint from a Data Subject relating to processing of Personal Data by an HP BCR Company; or
  (d) where Personal Data is processed by an HP BCR Company located outside of the EU on behalf of an HP BCR Company in the EU, the Competent Supervisory Authority for the HP BCR Company in the EU.

Relevant Supervisory Authority – Means the Supervisory Authority or court as set out below:

Factor	*Supervisory Authority*	*Court*
The European Country where the EU Data Subject has his or her habitual residence	√	√
The European Country where the EU Data Subject has his or her place of work	√	
The European Country where the Original Data Exporter has an establishment		√