

Cisco Systems - UK Binding Corporate Rules Summary (Controller)

1. Introduction:

Cisco is committed to respecting and protecting the privacy of its workers, customers, business partners, and other individuals whose Personal Data Cisco processes. Cisco Group Companies have entered into UK Binding Corporate Rules (“Cisco’s UK BCRs”) to provide appropriate safeguards for the processing of UK Personal Data and to ensure that such data is protected throughout Cisco. The UK BCRs apply where Cisco processes UK Personal Data, as a Data Controller, that is either Business Personal Data or HR Personal Data. A summary of Cisco’s UK BCRs is provided below (the “Summary”).

Please see Section 7 for a glossary of the terms used in this Summary.

A list of the Cisco Group Companies and countries to which Personal Data may be transferred can be found [here](#). UK Personal Data will only be transferred to a Cisco Group Company in reliance on Cisco’s UK BCRs where that Cisco Group Company is a member of Cisco’s UK BCRs (a “UK BCR Member”). If the Cisco Group Company in question is not a UK BCR Member, then the transfer will be carried out in reliance on an alternative transfer mechanism under UK Data Protection Law.

2. Categories of UK Personal Data & Data Subjects

2.1. Business Personal Data

Cisco processes Business Personal Data relating to individuals who are customers, online visitors, students (e.g., Networking Academy participants), and business partners, including resellers, vendors and alliance partners (or who represent organizations who are any of the above). The type of Business Personal Data that Cisco processes will depend on the business context and the purpose for which the data was collected. It may include:

- a) contact, subscription, registration, online identifiers, and social media details;
- b) financial information (e.g., bank account details);
- c) details of an individual’s business and other interests and opinions (e.g., where information is held in a Customer Relationship Management database); and
- d) other administrative data relating to Cisco’s business operations to the extent such data consists of Business Personal Data.

2.2. HR Personal Data

Cisco processes HR Personal Data about individuals who are:

- a) current and former Cisco Workers, including retirees;
- b) Cisco Candidates and other prospective Cisco employees, such as those joining Cisco as a part of an acquisition;
- c) dependents and beneficiaries of current and former Cisco Workers and individuals who should be contacted in the case of an emergency; and

- d) students when engaged as part of their study or on work experience (e.g. internship) at Cisco.

The categories of HR Personal Data that Cisco may process about the individuals listed above will depend on the nature of the individual's relationship with Cisco, and may include:

- a) contact details;
- b) financial information (e.g. bank account details, etc.);
- c) recruitment information (e.g. resume, etc.);
- d) employment administration information;
- e) information relating to an individual's use of Cisco assets, such as computers, cell phone, etc., including user IDs and passwords;
- f) information relating to the administration of employee benefits;
- g) information relating to an individual's use of a corporate credit card, including relevant transaction records;
- h) information about an individual's business travel;
- i) other personal information that may be disclosed during the course of a business relationship with Cisco.

3. Purpose of processing

3.1. Business Personal Data

Cisco collects, processes, and uses Business Personal Data for a variety of business reasons, such as to:

- a) form contracts with vendors, partners, and suppliers;
- b) fulfil orders;
- c) perform our contractual requirements and obligations;
- d) protect our legal rights;
- e) fulfil our legal obligations;
- f) provide and administer our services and solutions;
- g) manage relationships;
- h) successfully run our operations;
- i) promote and improve our goods and services; and
- j) provide customer services.

If Cisco processes Business Personal Data in more than one capacity (such as where an individual is a customer and a user of our services) then more than one processing purpose may apply. The following are examples of the purposes for which Cisco may process Business Personal Data:

- a) negotiating, conducting, and performing contracts with customers, suppliers, and other third parties (including the provision of financial services and advice);
- b) conducting due diligence and background checks;
- c) processing orders and payments;
- d) providing product functionality, services, and other business solutions, and customer support; and
- e) creating, enhancing, and managing Cisco accounts, records, and business relationships.

3.2. HR Personal Data

Cisco processes HR Personal Data in order to select, set up relationships with, maintain and administer

our workforce; run our operations; and ensure the safety and protection of Cisco Workers, Cisco Candidates and our resources, in the context of its relationship with Cisco Workers and Cisco Candidates.

3.3.Purpose Limitation

Cisco shall not process UK Personal Data for a purpose which is incompatible with the purposes for which it was originally collected unless:

- a) such UK Personal Data is processed in an anonymous or aggregate form; or
- b) consent is obtained from the individuals concerned; or
- c) a separate legal basis for processing is established.

4. Individual rights

In accordance with UK Data Protection Law, an individual who has satisfactorily established their identity to Cisco may exercise the rights listed below in relation to UK Personal Data that Cisco processes about them. Cisco shall allow individuals to exercise these rights in accordance with the legal conditions to which the exercise of such rights is subject.

4.1.Access, Rectification and Portability

Cisco shall provide an individual with the right to access and, where necessary, the ability to rectify their UK Personal Data. In addition, to the extent processing is based on consent or contract, and carried out by automated means, Cisco shall, upon reasonable request, provide to an individual a copy of their UK Personal Data in a structured and commonly used machine-readable format in accordance with UK Data Protection Law.

4.2.Erasure

Cisco shall provide individuals with the right to request that their UK Personal Data be erased, as such right is granted, interpreted, and limited by UK Data Protection Law, including in circumstances where:

- a) the UK Personal Data is no longer necessary for the purpose for which it was collected;
- b) the individual withdraws any consent on which the processing of their UK Personal Data was based;
- c) the individual successfully exercises the right to object to processing; or
- d) the processing of an individual's UK Personal Data is not in accordance with Cisco's UK BCRs.

4.3.Objection

Cisco shall provide individuals with the right to object to the processing of their UK Personal Data in circumstances where:

- a) Cisco is unable to demonstrate that its legitimate interests in processing an individual's UK Personal Data override the interest, rights, and freedoms of the individual;
- b) the individual would be subject to a decision based solely on automated processing (including profiling), which produces legal effects concerning them or similarly significantly affects them;
- c) the individual's UK Personal Data is processed for direct marketing purposes, including profiling to the extent it is used for such direct marketing purposes.

4.4.Restriction

Cisco shall provide individuals with the right to restrict the processing of their UK Personal Data in the

following circumstances:

- a) the individual contests the accuracy of their UK Personal Data and Cisco requires a period of time to verify the accuracy of their UK Personal Data;
- b) the processing is unlawful, and the individual opposes the erasure of the UK Personal Data and requests the restriction of its use instead;
- c) Cisco no longer needs the UK Personal Data for the purposes of processing, but the UK Personal Data is required by the individual for the establishment, exercise, or defense of legal claims; and
- d) the individual has objected to processing and there is a period pending verification of whether the legitimate grounds of Cisco override those of the individual.

4.5. Automated Decision-making

Cisco will not evaluate or take decisions about individuals that produce legal effects or which similarly significantly affects individuals based solely on the automated processing of their UK Personal Data. The exception to this is:

- a) where the processing is authorized under UK Data Protection Law;
- b) the decision is necessary for entering into a contract between the individual and Cisco, or
- c) the individual has given consent; in which case Cisco will put in place measures to protect the rights and freedoms and legitimate interests of individuals.

5. Complaints & Contact Details

Individuals whose Personal Data is processed by Cisco under the terms of Cisco's UK BCRs (as described in this Summary) can contact Cisco by submitting a request via the Privacy Request form at <https://privacyrequest.cisco.com>.

Details of the respective complaints procedures are provided below. If the individual is unsatisfied by Cisco's response (including where Cisco has rejected the complaint), the individual may exercise their enforcement rights (see section 6 below). In relation to UK Personal Data, individuals can also make a complaint directly to the ICO via their [website](#).

5.1. Business Personal Data

Details of how to make a complaint in relation to Cisco's processing of Business Personal Data are provided to individuals in Cisco's [Online Privacy Statement](#). Cisco will respond to any inquiries and complaints without undue delay and, in any event, within one (1) month of the receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The individual will be informed of such extension within one month of receipt of the request, together with the reasons for the delay. If the complaint cannot be resolved by the relevant team, it shall be escalated to Cisco's Privacy Center of Excellence and/or Cisco Legal.

5.2. HR Personal Data

Cisco Workers can make a complaint in relation to Cisco's processing of their HR Personal Data by reporting the concern to their Human Resources representative or to the HR Data Privacy team directly. If the Cisco Worker does not feel comfortable reporting the concern to his/her Human Resources representative, or does not feel that the concern was resolved after it was reported to his/her Human Resources representative, the Cisco Worker may report the concern to the Ethics

Hotline, the HR Data Privacy Team or, the Privacy Request form at <https://privacyrequest.cisco.com>. Cisco Candidates can make a complaint in respect of the processing of their HR Personal Data via <https://privacyrequest.cisco.com>. Cisco will respond to any inquiries and complaints without undue delay and, in any event, within one month. Taking into account the complexity and number of requests, the period for responding may be extended by two further months. In cases where an extension is required, Cisco will inform the Individual that additional time is needed to respond.

6. Enforcement

An individual can enforce the following elements of Cisco's UK BCRs in respect of UK Personal Data (note: the references below are to the relevant sections of Cisco's BCR-C Policy Documents as amended by the UK BCR-C Addendum):

- The data protection principles (see 'Application of the Data Protection and Privacy Principles'; 'Application of the Privacy Principles to European HR Data');
- Transparency and easy access to the UK BCRs (see 'Communicating this Policy'; 'Communication of this European HR Policy');
- Individual rights (see 'Individual Rights');
- National legislation preventing respect of the UK BCRs (see 'Conflict of Laws' and 'Local Law Requirements and Disclosure Requests' as amended by the UK BCR-C Addendum);
- Right to complain through the internal complaint mechanism (see 'Complaint Handling for Business Personal Data'; 'Grievance Mechanism');
- Cooperation with the ICO (see 'Co-operation with European Data Protection & Privacy Authorities'; 'Co-operation with Data Privacy Authorities' as amended by the UK BCR-C Addendum); and
- The right to lodge a complaint with the ICO and before the courts of England and Wales (see 'Third Party Beneficiary Rights' as amended by the UK BCR-C Addendum).

An individual can enforce their rights against Cisco as described in this Summary by direct recourse to the courts or other judicial authority. In respect of UK Personal Data, individuals can seek redress (including compensation, where appropriate) for a breach of their rights under Cisco's UK BCRs by direct recourse to the courts of England and Wales.

In respect of claims concerning UK Personal Data, an individual may enforce their rights as provided in this Summary against: (i) the Cisco Group Company in breach of Cisco's UK BCRs (if that company is in the UK), or (ii) the Lead UK Cisco Group Company (if the breaching Cisco Group Company is outside the UK). The relevant Cisco Group Company (as determined by the application of scenario (i) or (ii) above) will take the necessary remedial actions and assume liability for the damages caused to the individual as a result of the breach of Cisco's UK BCRs, unless Cisco can demonstrate that the allegedly breaching Cisco Group Company was not responsible for the breach of Cisco's UK BCRs giving rise to those damages or that no such breach took place. Where the breaching Cisco Group Company is outside the UK, the Lead UK Cisco Group Company will bear the burden of proof to show that the Cisco Group Company was not responsible for the breach or that no such breach took place, and will assume liability for payment of any compensation (following all due process).

7. Definitions

Business Personal Data	UK Personal Data relating to individuals who are customers, online visitors, students (e.g., Networking Academy participants), and business partners, including resellers, vendors and alliance partners (or who represent organizations who are any of the above). In other words, all non-HR related UK Personal Data.
Cisco	All Cisco Group Companies. A list of the Cisco Group Companies and countries to which Personal Data may be transferred can be found here .
Cisco Group Company	A company controlled, directly or indirectly, by Cisco Systems, Inc.
Cisco Systems, Inc.	Cisco Systems, Inc. c/o Corporation Service Company, 251 Little Falls Drive Wilmington, Delaware 19808-1674 Official registration number (if any) (company number or similar identifier): DE File Number 3704171
Cisco's UK BCRs	Cisco's BCR-C Policy Documents as extended by the terms of Cisco's UK BCR-C Addendum to include restricted transfers subject to UK Data Protection Law.
UK BCR-C Addendum	The UK addendum to Cisco's BCR-C Policy Documents, which is comprised of: (i) version C.1.0 of the UK BCR Addendum, as issued by the ICO on 19 December 2023 and (ii) this UK BCR Summary.
Cisco's BCR-C Policy Documents	(i) Business Personal Data Protection and Privacy Policy, including Annex 1: European Business Personal Data; (ii) European HR Data Protection Policy; and (iii) Global Personal Data Protection & Privacy Policy.
Cisco Worker ¹	A party (person) who provides personal services to Cisco in exchange for payment. This includes employees and contractors.
Cisco Candidate	A person who is of interest for a job opportunity at Cisco, but may not have applied for a specific job.
Data Controller	An entity which alone or jointly determines the purpose for which, and

¹ Any reference to 'Cisco Worker or Candidate' in this Summary is only for the purpose of the operation of this UK BCR Summary and is not intended to and does not, independently of the individual expressly being stated to be an employee of Cisco, in any way indicate or give rise to an employment relationship between the 'Cisco Worker or Candidate' as referenced, and Cisco. The inclusion of applicants in the definition of 'Cisco Candidates' should not be taken as a representation by Cisco that any of those Individuals have been, are being, or will be, offered a job by Cisco.

	the manner in which, Personal Data is being processed.
HR Personal Data	<p>UK Personal Data processed by or on behalf of Cisco in the context of the Cisco Worker's or Candidates' actual or potential working relationship with Cisco. A Cisco Worker or Candidate is 'identifiable' if they can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. Cisco human resources data includes each of the following:</p> <ul style="list-style-type: none"> • Cisco Worker or Candidate Company Identification Data - Data generated and/or collected solely for the purpose of identifying a Cisco Worker in the performance of their duties for Cisco. • Cisco Worker or Candidate Contextual Data - Data generated and/or collected which identifies or describes the performance, compensation or other similar information which provides additional information about the worker, their background and family. • Cisco Worker or Candidate Personal Identification Data - Data generated and/or collected which identifies or describes non-Cisco identifiers related to the workers' bank, governmental or other accounts.
ICO	The Information Commissioner (including their statutory successors).
Lead UK Cisco Group Company	<p>Cisco International Limited 9-11 New Square, Bedford Lakes, Feltham, Middlesex, United Kingdom, TW14 8HA Company number: 06640658</p>
Personal Data	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 a name, an identification number, location data, an online identifier or to one or more factors specific to the identity of that natural living person.
UK GDPR	The General Data Protection Regulation 2016/679 of 27 April 2016 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act of 2018.
UK Personal Data	Business Personal Data and HR Personal Data that is subject to UK Data Protection Law, or which was collected in circumstances where it was subject to UK Data Protection Law.
UK Data Protection Law	All applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data

	Protection Act 2018 (and regulations made thereunder); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended, along with any replacement laws or regulations.
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Start Date: [X]