IIJ UK BCR-C

（Controller Policy）

Version 1.0

14th March 2025

Internet Initiative Japan Inc.

Version No.	Revision Date	Revision Reason & Details	Approval	Creation/Revision
Ver. 1.0	14th March 2025	Initial Version	Sumiya	IIJ Chief Privacy Office

Table of Contents

1. Introduction

1.1. Purpose

In order to comply with the UK General Data Protection Regulation ("**UK GDPR**") and any applicable implementing laws, regulations and guidance (including, for the avoidance of doubt, the Data Protection Act 2018) (collectively "**UK Data Protection Law**"), as well as to guarantee the highest level of protection for the Personal Data the IIJ Business Entities (a list of which members and their contact details is available at Annex 1) process (process means conducting of any operation or set of operations which is performed on Personal Data or on sets of Personal Data, 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, blocking, restriction, erasure or destruction; the same hereinafter) as a Data Controller, IIJ has adopted these Binding Corporate Rules (the "**IIJ UK BCR-C**" or these "**BCRs**").

1.2. Scope

1.2.1. Geographic Scope

The IIJ UK BCR-C apply to the processing of following Personal Data that are transferred (transfer means the disclosure, transmission or making available of Personal Data to an entity in a Third Country or to an international organization; the same hereinafter) directly or indirectly from one of the IIJ Business Entities acting as a Data Controller to another IIJ Business Entity acting as a Data Controller or a Data Processor outside the UK, regardless of the nature of the Personal Data being processed. Such transfer includes onward transfers to other IIJ Business Entities located outside the United Kingdom ("**UK**").

- Personal Data being processed in the context of the activities of the IIJ Lead Business Entity; and
- Personal Data of Data Subjects who are in the UK being processed by the IIJ Business Entities not established in the UK, where the processing activities are related to the offering of products or services, irrespective of whether a payment of the Data Subject is required, to such Data Subjects in the UK.

The geographic scope of the IIJ UK BCR-C is comprised of the UK and countries in which IIJ Business Entities are present.

1.2.2. Standing vis-à-vis IIJ Business Entities

The IIJ UK BCR-C Policy is a group policy legally binding vis-à-vis all IIJ Business Entities by means of an Intra-Group Agreement to which the IIJ Business Entities are parties. Each IIJ Business Entity has a duty to respect and comply with the IIJ UK BCR-C Policy.

1.2.3. Standing vis-à-vis Employees

The IIJ UK BCR-C Policy is a group policy which Executives and Others are bound to respect, as provided for in their employment contracts. In order for Executives and Others to understand the details of the IIJ UK BCR-C Policy and comply with it, each IIJ Business Entity's Chief Privacy Office will provide appropriate information and necessary consultations. Furthermore, Executives and Others are compelled to participate in periodical trainings described in Section 11.

1.3. Document Retention and Distribution

The IIJ UK BCR-C Policy is made available to Executives and Others and will be communicated to customers and the Data Subjects upon request as specified in Section 4.

1.4. Related Documents

The IIJ UK BCR-C Policy also comprises the Annexes listed in Section 18 which describe the procedures that guarantee the effective implementation of the IIJ UK BCR-C Policy.

1.5. Keywords

The following definitions apply for the purposes of the present BCR Policy:

Term	Definition
Commissioner	The Information Commissioner appointed under Part 2, Schedule 12, of the Data Protection Act 2018 (as amended).
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
Data Controller	Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. For purposes of the IIJ UK BCR-C Policy, Data Controller refers to one of the

Term	Definition
	IIJ Business Entities.
Data Processor	Natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller. For purposes of the IIJ UK BCR-C Policy, Data Processor refers to one of the IIJ Business Entities.
Data Subject	Identified or identifiable natural person whose Personal Data is processed.
DPO	Data Protection Officer at IIJ who is responsible for monitoring compliance with the IIJ UK BCR-C and data protection laws at a global level. If any events relevant to compliance with the IIJ UK BCR-C occur, the DPO shall report such events to both the President of IIJ and/or the board of directors, as appropriate.
Executives and Others	The persons who exercise control and supervision of the IIJ Business Entities and are engaged in the business operations, as well as all staff of IIJ Business Entities, including employees having an employment relationship (full-time employees; contract and other temporary employees; part-time employees, etc.), officers (Directors, Auditors, etc.); and seconded employees of IIJ Business Entities.
IIJ	Internet Initiative Japan Inc.
IIJ Business Entities or IIJ Business Entity	Companies to which the IIJ UK BCR-C apply and which have signed the Intra-Group Agreement referred to in Section 1.2.2, a list of which companies is available in Annex 1.
IIJ Business Entity's Compliance Department	Departments in charge of general legal affairs and compliance that are set up at each of the IIJ Business Entities, which may assist the IIJ Business Entity's Chief Privacy Office or the IIJ Business Entity's CPO with the application of and compliance with local laws.
IIJ Business Entity's Chief Privacy Office	Security control departments that are set up in each of the IIJ Business Entities. They have the role of ensuring the protection of Personal Data, as well as supervising security control in IIJ Business Entities. The IIJ Business Entity's Chief Privacy Office shall cooperate with the IIJ Business Entity's CPO, as well as with the IIJ CPO, in giving instructions to the

Term	Definition
	IIJ Business Entity's departments that process Personal Data, including guidance, implementation of risk assessments and internal audits. Each IIJ Business Entity's Chief Privacy Office shall consider appropriate technical and organizational security measure in the first stage of projects and in the course of processing Personal Data in order to ensure appropriate data protection in projects. Each IIJ Business Entity's Chief Privacy Office can seek advice from the IIJ CPO, if necessary.
IIJ Business Entity's CPO	The IIJ Business Entity's Chief Privacy Officer ("**CPO**") is appointed at each IIJ Business Entity by that IIJ Business Entity's President, and is responsible for the implementation and operation of the IIJ UK BCR-C in that IIJ Business Entity. The IIJ Business Entity's CPO is assisted by the IIJ Business Entity's Chief Privacy Office.
IIJ Chief Privacy Office	The security control department that is set up at IIJ. It has the role of ensuring global data protection as well as supervising the security control of all of the IIJ Business Entities.
IIJ Compliance Department	The department at IIJ in charge of general legal affairs and compliance at a global level.
IIJ CPO	CPO in IIJ whose responsibilities and authorities include: providing advice and assistance on the overall implementation and operation of the IIJ UK BCR-C for the IIJ Business Entities; supervising the overall implementation of the IIJ UK BCR-C by the IIJ Business Entities and reporting on such implementation to the DPO; ensuring that IIJ Business Entities are informed of the DPO's instructions and advice; assessing data processing activities reported for approval and conducting data processing impact assessments as appropriate; assessing Personal Data Transfers reported for approval and preparing the requisite documentation; preparing responses to Data Subject rights exercise where requested; assessing security incidents or Personal Data breaches and possible related regulatory obligations; and dealing with the Commissioner's investigations.
IIJ Group	The group of companies comprising of consolidated

Term	Definition
	subsidiaries of IIJ and equity method investees of IIJ, of which IIJ is the ultimate parent company
IIJ Internal Audit Office	Internal audit department that is set up at IIJ.
IIJ Lead Business Entity	Refers to IIJ Europe Limited, which is an IIJ Business Entity established and operating in the UK, and located at: 1st Floor 80 Cheapside London, United Kingdom EC2V 6EE.
IIJ UK BCR-C Policy or "this BCR Policy"	Collective term referring to this document and to the Annexes that are stipulated in Section 18, collectively setting out Personal Data protection policies which are adhered to by the IIJ Business Entities as a Data Controller for transfers or a set of transfers of Personal Data to a Data Controller or Data Processor in one or more Third Countries. The IIJ UK BCR-C Policy and the Intra-Group Agreement that makes the Policy binding upon the IIJ Business Entities constitute the IIJ UK BCR-C.
Personal Data	Any information relating to a Data Subject; a Data Subject 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 terms "personal information" and "personally identifiable information" shall have the same meaning as the term "Personal Data" in the context of the issues regulated in the IIJ UK BCR-C Policy.
Sensitive Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data and biometric data the processing of which can uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Third Country or Third Countries	Any country or territory outside the UK.
Third Party	Natural or legal person, Public Authority or Public Body,

Term	Definition
	excluding the Data Subject, any IIJ Business Entity (as Data Controller and/or Data Processor), and any persons who, under the direct authority of the Data Controller or the Data Processor, are authorised to process Personal Data (where Public Authority and Public Body are to be interpreted in accordance with Section 7 of the Data Protection Act 2018 and provision made under that Section).
Third Party Beneficiaries	Data Subjects and persons who may exercise their rights under the IIJ UK BCR-C, excluding the person who is defined as Third Party.
UK	The United Kingdom which consists of England and Wales, Northern Ireland and Scotland.
UK Data Protection Law	The UK GDPR together with applicable implementing laws, regulations, guidance and other data protection laws of the United Kingdom or of a part of the United Kingdom (including, for the avoidance of doubt, the Data Protection Act 2018), all as amended or replaced from time to time. In each case, such laws must provide appropriate safeguards for the rights and freedoms of Data Subjects.

2. General Principles of Personal Data Processing

General Principle. The principles set out in the IIJ UK BCR-C Policy shall be respected by IIJ Business Entities irrespective of national laws in Third Countries, except where local legislation includes more stringent requirements protecting Personal Data than those established under the IIJ UK BCR-C Policy. Where there are aspects of the IIJ UK BCR-C Policy that are subject to more stringent local legislation, the more stringent legislation will apply to these aspects.

Relationship between National Law and the IIJ UK BCR-C Policy. If an IIJ Business Entity has reasons to believe that any legal requirements to which it is subject in a Third Country prevents it from fulfilling its obligations under the IIJ UK BCR-C Policy, or would have a substantial effect on the guarantees provided by the IIJ UK BCR-C Policy, the person in charge of such IIJ Business Entity shall promptly inform the IIJ Lead Business Entity of the issue and seek support from that IIJ Business Entity's Chief Privacy Office by electronic mail or in writing. In case of doubt as to the application of the IIJ UK BCR-C Policy and local laws, and where these conflicts cannot be quickly resolved, the IIJ Business Entity's Chief Privacy Office will correspond with the Commissioner.

Further, if the IIJ Business Entity has reason to believe that legal requirements it may be subject to in Third Countries are likely to have a substantial adverse effect on the guarantees provided by the IIJ UK BCR-C Policy (including legally binding requests for disclosure of Personal Data by a law enforcement authority or state security body), the IIJ Business Entity will promptly and clearly inform the Commissioner about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure of Personal Data by the law enforcement or state security body, unless this is prohibited by a law enforcement authority (including obligations under criminal laws to preserve the confidentiality of a law enforcement investigation). In this regard, the IIJ Business Entity's CPO shall cooperate with the DPO to inform the Commissioner. If in specific cases the suspension and/or notification to the Commissioner are prohibited, the IIJ Business Entity will use its best efforts to obtain the right to waive such prohibition in order to communicate as much information to the Commissioner as it can and as soon as possible, and be able to demonstrate having done so. If, despite the IIJ Business Entity's best efforts, it is not in a position to notify the Commissioner, it will provide general information to the Commissioner at least once a year on the requests it receives (e.g., the number of applications for disclosure, type of data requested, requester if possible, etc.), in accordance with the procedure set out in Section 16. In any event, where the IIJ

Business Entity is obliged to provide Personal Data to a public authority, such transfer shall not concern a massive or disproportionate amount of Personal Data, and shall not be indiscriminate in such a manner as to go beyond what is necessary in a democratic society.

In addition to the abovementioned provisions, regarding the obligation to consult with the Commissioner if there are doubts as to the interpretation of local laws which cannot be quickly resolved, each IIJ Business Entity's Chief Privacy Office and/or IIJ Chief Privacy Office shall also seek the advice of the relevant IIJ Business Entity's Compliance Department and/or IIJ Compliance Department, the DPO, or an outside counsel, and shall ensure compliance with local laws.

Responding to Support Requests. Each IIJ Business Entity's Chief Privacy Office that has received a support request for the issue mentioned above shall take measures to address the issue within one (1) month, and if it is not able to take any measures for the problem within that period, the IIJ Business Entity's Chief Privacy Office shall escalate it to IIJ Chief Privacy Office, and ultimately to the DPO. The IIJ Chief Privacy Office shall, in cooperation with the DPO, take action to resolve that issue within two (2) months of having received such escalation.

2.1. Legal Basis for Personal Data Processing

The IIJ Business Entity as a Data Controller can carry out Personal Data Processing only where:

- the Data Subject has given Consent to the processing of his or her Personal Data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the Data Subject is a party, or in order to take steps at the request of the Data Subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the Data Controller is subject;
- processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; or

- processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

2.2. General Principles Relating to Processing of Personal Data

The IIJ Business Entity shall be responsible for, and be able to demonstrate compliance with, the following principles:

- **Lawfulness, Fairness and Transparency:** The IIJ Business Entity shall process Personal Data lawfully, fairly and in a transparent manner in relation to the Data Subject.
- **Purpose Limitation:** The IIJ Business Entity may process Personal Data only for specified, explicit and legitimate purposes, and not for other purposes, unless (i) the new purpose is compatible with the initial purposes, taking into account the factors enumerated in Article 6(4) of the UK GDPR, or (ii) the Data Subject consents to the further processing.
- **Data Minimisation:** The IIJ Business Entity shall ensure that Personal Data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** The IIJ Business Entity shall ensure that Personal Data are accurate and, where necessary, kept up to date. The IIJ Business Entity will take every reasonable step to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage Limitation:** The IIJ Business Entity shall keep Personal Data for no longer than is necessary for the purposes for processing of the Personal Data.
- **Integrity and Confidentiality:** The IIJ Business Entity shall process Personal Data under appropriate security countermeasures including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organisational measures according to Personal Data protection policy.

2.3. Collection of Personal Data

Where an IIJ Business Entity collects Personal Data relating to a Data Subject from the Data Subject, the IIJ Business Entity shall, at the time when Personal Data are obtained,

provide the Data Subject with all of the following information:

- the identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative and DPO;
- the purposes of the processing for which the Personal Data are intended, as well as the legal basis for the processing;
- if processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party, the legitimate interests pursued by the Data Controller or a Third Party;
- the recipients or categories of recipients of the Personal Data, if any;
- where applicable, the fact that the Data Controller intends to transfer Personal Data to a Third Country or international organisation and the existence or absence of relevant adequacy regulations under section 17A of the Data Protection Act 2018. In the latter case, the IIJ Business Entity shall also refer, when required to do so by the UK Data Protection Law, to the appropriate or suitable safeguards and the means to obtain a copy thereof or where they have been made available.

In addition to the information referred to above, the IIJ Business Entity acting as the Data Controller shall, at the time when Personal Data are obtained, provide the Data Subject with the following further information necessary to ensure fair and transparent processing:

- the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the Data Controller access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
- where the processing is based on the Consent of the Data Subject, as provided for in the UK Data Protection Law, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of processing based on Consent before its withdrawal;
- the right to lodge a complaint in accordance with the procedure set out in Section 5 and Annex 5, and/or with the Commissioner;

- whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such Personal Data;
- the existence of automated decision-making, including profiling, referred to in the UK Data Protection Law and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

The information referred to in the previous provisions will be provided in a clear and comprehensive way, usually by means of an easily accessible fair processing statement (e.g. for employees, in the handbook or on the intranet; for customers, it will make such notice available at all points where it collects Personal Data directly from Data Subjects).

When an IIJ Business Entity does not collect Personal Data directly from the Data Subject, it shall provide the Data Subject with the below additional information:

- the categories of Personal Data concerned;
- from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources.

The IIJ Business Entity should provide this information:

- within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are processed;
- if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject;
- if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

When contemplating the use of collected Personal Data for a different purpose than the one previously communicated to the Data Subject, the Data Subject will be provided with information relating to such purpose as well as with all relevant additional information prior to initiating the processing.

The IIJ Business Entity will follow this Section 2.3, unless there is a legal basis under UK domestic law for not doing so (for example, where the processing is based on UK

domestic law constituting a necessary and proportionate measure in a democratic society to safeguard national security or defence, or where the processing is for the prevention or detection of criminal offenses, taxation purposes, judicial proceedings or other objectives set forth in Article 23(1) UK GDPR).

2.4. Processing the Personal Data of Children

Where processing is based on Consent, in relation to the offer of information society services (but excluding preventative and counselling services) directly to a child below the age of thirteen (13) years (or a lower age, as set by the laws of any part of the UK), processing of Personal Data shall be possible only if and to the extent that Consent is given or authorised by the holder of parental responsibility over the child. The IIJ Business Entity shall make reasonable efforts to verify in such cases that Consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

For the purposes of the IIJ UK BCR-C Policy, "information society service" means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, in line with the definition of the term in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council.

2.5. Processing Sensitive Data

Each IIJ Business Entity can process Sensitive Data only where:

- the Data Subject has given explicit Consent to the processing of this Sensitive Personal Data for one or more specified purposes, except where the applicable UK domestic law provides that the processing of such data is prohibited and that the prohibition may not be lifted by the Data Subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by UK domestic law or a collective agreement pursuant to UK domestic law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;

- processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the Consent of the Data Subjects;
- processing relates to Personal Data which is manifestly made public by the Data Subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of UK domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of UK domestic law or pursuant to contract with a health professional and subject to the conditions, safeguards and obligations of secrecy provided by the applicable UK domestic law or rules established by competent bodies of the United Kingdom or a part of the United Kingdom;
- processing is necessary for reasons of public interests in the area of public health, on the basis of UK domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy; or
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the

applicable UK domestic law (and specifically, in accordance with Article 89(1) of the UK GDPR as supplemented by section 19 of the Data Protection Act 2018 and based on UK domestic law) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

In the event that an IIJ Business Entity processes Personal Data relating to criminal convictions and offenses or related security measures pursuant to one of the legal bases identified in Section 2.1 of this BCR Policy, such processing must be authorized by UK domestic law providing for appropriate safeguards for the rights and freedoms of Data Subjects, as set forth in Article 10 of the UK GPDR.

2.6. Security

2.6.1 General Security Policies

Each IIJ Business Entity shall implement appropriate technical and organisational security measures in order to protect Personal Data from unauthorized or unlawful processing and against accidental loss, destruction or damage, in particular where processing involves transmission of Personal Data over a network, and against all other unlawful forms of processing. To this end, each IIJ Business Entity shall comply with the requirements in the IIJ Group Security Policy, as revised and updated from time to time, together with any other security procedures relevant to a business area or function. Each IIJ Business Entity will implement and comply with breach notification policies as required by the UK Data Protection Law. Furthermore, each IIJ Business Entity will ensure that providers of services to that IIJ Business Entity also adopt appropriate and equivalent security measures by concluding contracts which oblige such providers to adopt such measures and any other means.

2.6.2 Personal Data Breach

Where there is a breach of security or confidentiality that affects the Personal Data of individuals, the IIJ Business Entity shall notify the breach to the Commissioner without undue delay and, where feasible, within 72 hours after becoming aware of the Personal Data breach, unless such breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Commissioner is not made within 72 hours, it shall be accompanied by reasons for the delay.

Where the Personal Data breach is likely to result in a high risk to the rights and freedoms of the Data Subjects, the IIJ Business Entity shall notify, without undue delay, the data breach to the IIJ Lead Business Entity, the IIJ CPO, the DPO and the Data Subjects concerned.

The IIJ Business Entity's CPO will document such breach (including the facts of the breach, the effects, and the remedial action taken), and report to the IIJ CPO, and ultimately the DPO. IIJ shall make such materials available to the Commissioner upon request.

2.7. Procedures Ensuring Compliance with the Principles of Section 2

Annex 2 "Scope of Personal Data - Procedures for Identifying Personal Data" and Annex 3 "Procedures Regarding Risk Analyses, etc. Relating to Personal Data" set forth processes and procedures which will ensure compliance with the principles stipulated in Section 2 of this BCR Policy.

3. Transfer of Personal Data

In order to provide IT solutions to meet the needs of their customers' overseas establishments and in order to enable and facilitate HR management for IIJ employees, IIJ Business Entities will transfer Personal Data of customers (and their customers), suppliers and service providers, and of Executives and Others, to other IIJ Business Entities or Third Party processors appointed by IIJ Business Entities, both within and outside of the UK. For the avoidance of doubt, transfer of Personal Data to external processors outside of the UK may be conducted only where the conditions laid down in Articles 45, 46 or 49 of the UK GDPR are complied with by the relevant IIJ Business Entities and external processors.

The types of Data Subjects, categories of Personal Data and purposes for processing (including transfers) which are covered by this BCR Policy include the following:

Employee data (name, gender, address, phone number, email address, date of birth, work experience, salary)

- Purpose of processing: To conduct personnel management of employees of IIJ Business Entity.
- Affected Data Subjects: employees of IIJ Business Entities
- Types of processing:
  (1) The employee who works at the site in the UK or the personnel manager at the site in the UK sends by email Personal Data of the employees working at the entities in the UK, to the personnel manager at the IIJ Business Entity outside the UK;
  (2) HR manager of IIJ Business Entity outside the UK stores the received employee data in an area accessible only to the concerned parties;
  (3) the personnel manager in charge of the IIJ Business Entities outside the UK reviews and processes employee data for personnel management (training, personnel evaluation, transfer and promotion, placement management, etc.).
- Countries to which employee data is or may be transferred: Germany, Japan, Thailand, Vietnam, Singapore, Malaysia, China, Hong Kong, Indonesia and United States of America.

IIJ supplier and service provider data (company name, office address, contact details of person in charge (name, department position, phone number, email address))

- Purpose of processing: To provide IT solutions that meet the needs of customers'

overseas offices.

- Affected Data Subjects: suppliers and service providers of IIJ Business Entities
- Types of processing:
  (1) Case manager of IIJ Business Entity receives Personal Data of persons in charge of suppliers or service providers from themselves via business card or email;
  (2) Case manager of IIJ Business Entity digitalizes or stores such data in the area accessible only to the parties concerned;
  (3) The parties concerned in IIJ Business Entity may browse Personal Data of the suppliers' or service provider's personnel stored for supplier registration, purchase order process, purchase invoicing.
- Countries to which IIJ supplier and service provider data is or may be transferred: Germany, Japan, Thailand, Vietnam, Singapore, Malaysia, China, Hong Kong, Indonesia and United States of America.

Customer data (company name, office address, contact details of person in charge (name, department position, phone number, email address))

- Purpose of processing: To provide IT solutions that meet the needs of customers' overseas offices.
- Affected Data Subjects: customers of IIJ Business Entities
- Types of processing:
  (1) Case personnel in charge of IIJ Business Entity receive customer data from customers by business card or email;
  (2) Case manager of IIJ Business Entity digitalizes or stores such data in the area accessible only to the parties concerned;
  (3) The parties concerned of the IIJ Business Entity store the data and browse and process the stored customer data for quotation, order receipt, purchase, billing and marketing.
- Countries to which customer data is or may be transferred: Germany, Japan, Thailand, Vietnam, Singapore, Malaysia, China, Hong Kong, Indonesia and United States of America.

Data transfers are carried out by way of transmission of electronic data or data in paper, or transportation of electronic memory media.

In order to fulfil certain of the IIJ Group’s processing purposes, Personal Data to which

UK GDPR applies is transferred to non-UK countries or territories (including onward transfers between such non-UK countries or territories) for necessary functions, which may include: customer services, to provide IaaS and email outsourcing services, to provide human resources management, or for announcements on personnel changes and recruitment.

To ensure that the level of protection provided to the Personal Data is equalised throughout all IIJ Business Entities, we make the following stipulations regarding transfer of such Personal Data between IIJ Business Entities (except for transfers within the UK).

3.1. Personal Data Transfer from an IIJ Business Entity Acting as a Data Controller Located Within or Outside the UK to an IIJ Business Entity Located Outside the UK

Where an IIJ Business Entity, acting as a Data Controller, transfers Personal Data to which UK GDPR applies to another IIJ Business Entity (acting as Data Controller or Data Processor) located outside the UK, the transfer of the Personal Data is covered by the IIJ UK BCR-C Policy (for the avoidance of doubt, such transfer of Personal Data covered by the IIJ UK BCR-C Policy includes onward transfers between such non-UK countries or territories).

Where the IIJ Business Entity, acting as Data Controller, shares Personal Data with an IIJ Business Entity as a Data Processor, the IIJ Business Entity acting as Data Controller shall put in place an agreement with the IIJ Business Entity as a Data Processor that at minimum meets the requirements of Article 28(3) of the UK GDPR.

3.2. Personal Data Transfer from an IIJ Business Entity Acting as a Data Controller, Located Within or Outside of the UK to a Third Party Located Within or Outside of the UK

Any time an IIJ Business Entity, acting as a Data Controller, permits a Third Party to process Personal Data to which the UK GDPR applies, it shall (i) ensure that the Third Party is bound by law to appropriate duties of confidentiality and data security at least equal to those required by the UK Data Protection Law; and (ii) put in place a contract or other legal act under UK domestic law which is binding upon such Third Party with regard to the IIJ Business Entity, and which at minimum meets the requirements of Article 28(3) of the UK GDPR.

In the event that a Third Party processor engages another Third Party processor for carrying out specific processing activities on behalf of the IIJ Business Entity, it shall impose upon such subsequent Third Party processor by way of contract or other legal act under UK domestic law, the same data protection obligations as set forth under Article 28(3) of the UK GDPR. The Third Party processor shall remain fully liable to the IIJ Business Entity for the performance of the subsequent Third Party processor's obligations.

If an IIJ Business Entity, acting as a Data Controller, transfers Personal Data to a Third Party located outside the UK, the IIJ Business Entity transferring the Personal Data shall ensure compliance with Section 3 of this BCR Policy and shall either (i) rely on adequacy regulations under section 17A of the Data Protection Act 2018 (according to Article 45 of the UK GDPR), (ii) ensure that it executes the appropriate standard data protection clauses with such Third Party which are specified in regulations made by the Secretary of State under section 17C of the Data Protection Act 2018 and for the time being in force or specified in a document issued (and not withdrawn) by the Commissioner under section 119A of the Data Protection Act 2018 and for the time being in force (in each case, according to Article 46 of the UK GDPR), (iii) put in place another appropriate safeguard pursuant to Article 46 or 47 of the UK GDPR, or (iv) ensure that a derogation according to Article 49 of the UK GDPR applies.

***3.3. Personal Data Transfer from Data Controller** Located Within or Outside the UK to an IIJ Business Entity Located Outside the UK*

[Section intentionally blank in IIJ UK BCR-C Policy]

3.4 Personal Data Transfer from an IIJ Business Entity Acting as a Data Processor Located Within or Outside the UK to an IIJ Business Entity Located Within or Outside the UK

[Section intentionally blank in IIJ UK BCR-C policy]

3.5. Personal Data Transfer from an IIJ Business Entity acting as a Data Processor Located Within or Outside the UK to External Entities Located Within or Outside the UK

[Section intentionally blank in IIJ UK BCR-C Policy]

4. Rights of Data Subject

4.1. Right of Access by the Data Subject

If an IIJ Business Entity has been asked, by a Data Subject, for access to the Personal

Data concerning him or her that the IIJ Business Entity processes as a Data Controller, it shall handle that request in accordance with the procedure referred to below. This includes: (i) informing the Data Subject of whether IIJ Business Entities hold and process their Personal Data; (ii) providing the Data Subject with a description of their Personal Data that is processed, the purposes thereof and any recipients (or categories of recipients) to whom the Personal Data may be disclosed; (iii) where possible, the envisaged period for which the Personal Data is store, or if not possible, the criteria used to determine that period; (iv) providing the Data Subject with a copy of their Personal Data that is held and processed, in a format that can be reasonably understood; (v) the existence of the right to request rectification or erasure of Personal Data, restriction of processing or to object to processing; (vi) the right to lodge a complaint with the Commissioner; (vii) where the Personal Data are not collected from the Data Subject, any available information as to their source; (viii) the existence of automated decision-making, if applicable, including profiling, with meaningful information about the logic, significance and envisaged consequences of such processing, (ix) informing the Data Subject of the appropriate safeguards pursuant to Article 46 of the UK GDPR. where the Personal Data are transferred to a third country or to an international organisation.

4.2. Right to Rectification

If an IIJ Business Entity has been asked, by a Data Subject, to rectify Personal Data concerning him or her that it processes as a Data Controller, due to the reason that this Personal Data is incomplete or inaccurate, it shall handle that request without undue delay in accordance with the procedure referred to below.

4.3. Right to Erasure (Right to be Forgotten)

If an IIJ Business Entity has been asked, by a Data Subject, to erase Personal Data concerning him or her that it processes as a Data Controller, it shall erase such Personal Data where one of the following grounds applies:

- the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; However, it does not apply where the IIJ Business Entity acting as a Data Controller is not required, by the UK Data Protection Law, to erase the Personal Data (e.g. when that processing is necessary for reasons of public interest in the area of public health or for the establishment, exercise or defense of legal claims).

- the Data Subject withdraws Consent on which the processing is based as provided for in the UK Data Protection Law, and where there is no other legal ground for the processing;
- the Data Subject objects to the processing, as provided for in the UK Data Protection Law and there are no overriding legitimate grounds for the processing (except if the Personal Data relates to direct marketing).
- the Personal Data have been unlawfully processed;
- the Personal Data have to be erased for compliance with a legal obligation under UK domestic law to which the Data Controller is subject;
- where the Personal Data have been collected with a view to providing information society services directly to a child, the holder of parental responsibility withdraws the Consent or the Data Subject withdraws the Consent given or authorized by the holder of parental responsibility after having reached the age of digital Consent.

4.4. Right to Restriction of Processing

If an IIJ Business Entity has been asked by a Data Subject to restrict the processing of Personal Data that it carries out as a Data Controller, it shall respond positively to such a request where one of the following applies:

- the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Data Controller to verify the accuracy of the Personal Data;
- the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;
- the Data Controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defense of legal claims; or
- the Data Subject has objected to processing pursuant to the UK Data Protection Law, pending the verification whether the legitimate grounds of the Data Controller override those of the Data Subject.

4.5 Right to Data Portability

The Data Subject shall have the right to receive the Personal Data concerning him or her, which he or she has provided to the IIJ Business Entities, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data

controller without hindrance from the IIJ Business Entities to which the Personal Data have been provided, where:

(a) the processing is based on consent pursuant to the UK GDPR Article 6(1)(a) or Article 9(2)(a) or on a contract pursuant to UK GDPR Article 6(1)(b); and

(b) the processing is carried out by automated means.

In exercising the Data Subjects' right to data portability, the Data Subject shall have the right to have the Personal Data transmitted directly from the IIJ Business Entities to another data controller, where technically feasible. The right to data portability shall not adversely affect the rights and freedoms of others.

4.6 Right to Object

Data Subjects shall have the right to object, on grounds relating to his or her situation, at any time to processing of Personal Data, where the processing is based on Article 6(1)(e) or (f) of the UK GDPR, including profiling based on those provisions.

The IIJ Business Entity shall no longer process the Personal Data unless the IIJ Business Entity demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subjects or of the establishment, exercise or defence of legal claims.

Where Personal Data are processed for direct marketing purposes, the Data Subjects have the right to object at any time to processing of Personal Data for such marketing, including profiling (to the extent this is related to the direct marketing concerned).

4.7 Automated Individual Decisions

Data Subjects will have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, except:

1. Where this is necessary for entering into, or performing, a contract between the IIJ Business Entity and the Data Subject;
2. Where this is authorized by UK domestic law to which the IIJ Business Entity is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests.
3. Where this is based on the Data Subject's explicit Consent.

In the cases referred to in points 1 and 3 above, the Data Controller shall implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Data Controller, to express his or her point of view and to contest the decision. In the case referred to in point 2 above, the Data Controller shall implement suitable measures to safeguard the Data Subject's rights, freedoms, and legitimate interests, pursuant to section 14 of the Data Protection Act 2018, and regulations thereunder.

The automated decisions shall not be based on Sensitive Data, unless Article 9(2)(a) or (g) of the UK GDPR applies and suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests are in place.

Where decisions producing legal effects concerning an individual, or significantly affecting that individual, have been made by automated means, individuals will have the right to know meaningful information about the logic involved in the decision, and the significance and envisaged consequences of such processing for the Data Subject. The IIJ Business Entity will take necessary measures to protect the legitimate interests of individuals.

4.8. Right to Withdraw Consent

Data Subject shall have the right to withdraw his or her Consent at any time. If an IIJ Business Entity has been notified, by a Data Subject, that he or she withdraws Consent, it shall stop processing the Data Subject's Personal Data for the purposes for which the Consent was given. The withdrawal of Consent shall not affect the lawfulness of processing based on Consent before its withdrawal.

4.9. Right to Easy Access to IIJ UK BCR-C Policy

All Data Subjects have the right to have easy access to the IIJ UK BCR-C Policy. For this reason, the IIJ UK BCR-C Policy will be published in full (with the exception of Annex 7) on the website of IIJ (with a link to the BCR Policy provided in the IIJ Group Global Privacy Policy). For Executives and Others, the full IIJ UK BCR-C Policy will also be made available on the intranet.

4.10. Handling a Request from a Data Subject

If a request stipulated in this Section has been made, the IIJ Business Entity that is acting

as a Data Controller shall acknowledge receipt promptly, and provide a substantive response, without undue delay and at the latest within one (1) month and should include a statement of the possibility of lodging, at any time, a complaint or claim with the Information Commissioner or before a court or other competent judicial authority. In the event of a refusal to complete the request, such response should also include the reasons for not taking action. Requests and responses should be dealt with in accordance with the procedures stipulated in Annex 4 "Rules Regarding the Data Subject's Personal Data Rights."

If the request of the Data Subject is not approved, the Data Subject can enforce these rights in accordance with the procedures stipulated in Section 5 "Complaint Handling Procedures".

5. Complaint Handling Procedures

5.1. Direct Complaints

If a complaint has been filed by a Data Subject, alleging that their Personal Data has not been processed in accordance with the IIJ UK BCR-C Policy or the UK Data Protection Law, the IIJ Business Entity will handle that complaint in accordance with the procedures stipulated in Annex 5 “Procedures Regarding Complaints and Consultations Relating to Personal Data”.

Data Subjects may submit complaints by sending an email to the following address.
iijgroup-dpo-contact@iij.ad.jp
Complaints shall be dealt with, without undue delay and in any event within one (1) month, unless the complexity and number of requests mandates an extension by a maximum of two (2) further months, provided that affected Data Subjects are informed accordingly. The IIJ Chief Privacy Office is ultimately responsible for handling complaints from Data Subjects, and all complaints received by any Executives or Others at any of the IIJ Business Entities will be immediately forwarded to the IIJ CPO.

If the Data Subject has escalated its complaint for the reason that the IIJ Business Entity is not complying with the stipulations of this Section, the IIJ Business Entity will handle it in accordance with Section 6 “Liability towards Third Party Beneficiaries.”

Data Subjects may also submit a complaint or claim with the Commissioner or before a court or other competent authority in the UK as set out in Section 6.3, without first exhausting the IIJ Group’s complaint process.

5.2. Indirect Complaints

No description as a Data Controller

6. Liability towards Third Party Beneficiaries

6.1. Third Party Beneficiary Rights

It is acknowledged that the rights of Data Subjects whose Personal Data is processed by an IIJ Business Entity are enforceable under the IIJ UK BCR-C as Third Party Beneficiaries in the event of a breach by any IIJ Business Entity of *any* of its commitments herein, including:

- Purpose limitation (Section 2.2 of the IIJ UK BCR-C Policy),
- Data minimisation (Section 2.2 of the IIJ UK BCR-C Policy),
- Limited storage periods (Section 2.2 of the IIJ UK BCR-C Policy),
- Data quality and proportionality (Section 2.2 of the IIJ UK BCR-C Policy),
- Criteria for making the processing legitimate (legal bases) (Section 2.1 of the IIJ UK BCR-C Policy),
- Transparency and easy access to BCRs (Section 2.3 of the IIJ UK BCR-C Policy),
- Processing of Special Categories of Personal Data (Sections 2.4 and 2.5 of the IIJ UK BCR-C Policy),
- Rights of access, rectification, erasure, restriction and objection to the processing (Section 4 of the IIJ UK BCR-C Policy),
- Rights in case automated individual decisions are taken (Section 2.7 of the IIJ UK BCR-C Policy),
- Security and confidentiality (Section 2.6 of the IIJ UK BCR-C Policy),
- Requirements for onward transfers outside of the IIJ Group (Section 3 of the IIJ UK BCR-C Policy),
- National legislation preventing respect of BCRs (Section 2 of the IIJ UK BCR-C Policy),
- Right to complain through the internal complaint mechanism of the companies (Section 5 of the IIJ UK BCR-C Policy),
- Cooperation duties with the Commissioner (Section 8.2 of the IIJ UK BCR-C Policy),
- Liability and jurisdiction provisions (Section 6 of the IIJ UK BCR-C Policy),
- Data protection by design and by default (Section 9.2 of the IIJ UK BCR-C Policy).

Such rights include the right to judicial remedies and the right to obtain redress and, where appropriate, compensation for any damage. The Third Party Beneficiaries are entitled to submit a complaint or claim with the Commissioner and before a court or other competent authority in the UK as set out in Section 6.3.

6.2. Liability of IIJ Lead Business Entity

The IIJ Lead Business Entity shall in particular be responsible for and agree to take the necessary action to remedy the acts of non-UK IIJ Business Entities, including the duty to pay compensation for any material or non-material damages resulting from the violation of this BCR Policy by any non-UK IIJ Business Entities. In this regard, the IIJ Lead Business Entity shall assume ultimate liability for any such violations, as if the violation had been caused by the IIJ Lead Business Entity instead of the IIJ Business Entity outside the UK.

Further, the IIJ Lead Business Entity shall not be entitled to rely on a breach by an IIJ Business Entity of its obligations in order to avoid its own liabilities. However, if the IIJ Lead Business Entity can prove that the IIJ Business Entity outside the UK is not liable for the violation, it may discharge itself from any responsibility.

6.3. Liability and Enforceability in Case of the IIJ Business Entity Acting as a Data Controller

In the event of any violation of this BCR Policy, including by an IIJ Business Entity established outside the UK, the courts or other competent authorities in the UK shall have jurisdiction. The Data Subject may exercise their right to enforce the IIJ UK BCR-C, to obtain an effective judicial remedy, including the right to obtain redress and to receive compensation, before a court or other competent authority in the UK (see Section 180 of the Data Protection Act 2018). In addition, the Data Subjects have the right to lodge a complaint before the Commissioner.

6.4. Liability and Enforceability in Case of the IIJ Business Entity Acting as a Data Processor

[Section intentionally blank in IIJ UK BCR-C Policy]

6.5. Burden of Proof

The IIJ Lead Business Entity will have the burden of proof to demonstrate that any IIJ Business Entity outside the UK is not liable for any violation of the IIJ UK BCR-C which has resulted in the Data Subject claiming damages or remedy.

7. Liability of IIJ Business Entities acting as Data Processors vis à vis Data Controllers

[Section intentionally blank in IIJ UK BCR-C Policy]

8. Cooperation Mechanism

8.1. Cooperation with the Data Controller

[Section intentionally blank in IIJ UK BCR-C Policy]

8.2. Cooperation with the Commissioner

IIJ Business Entities shall cooperate and assist each other in order to handle requests or complaints from individuals or to comply with requests by the Commissioner in the context of investigations or inquiries.

IIJ Business Entities shall actively cooperate with the Commissioner in the performance of their tasks, and in particular, shall consider any communications or recommendations issued by the Commissioner and ensure adequate and timely replies to requests received from the Commissioner. IIJ Business Entities also accept, without restrictions, to be audited by the Commissioner to verify compliance with UK Data Protection Law, and with the IIJ UK BCR-C.

IIJ Business Entities shall make available to the Commissioner the results of verifications of compliance, which include data protection audits and methods for ensuring corrective actions to protect the rights and freedoms of Data Subjects.

IIJ Business Entities shall abide by the advice of the Commissioner on any issues regarding data protection, and shall comply with any formal decisions or notices issued by the Commissioner.

8.3. Notifications at the Time of Personal Data Breach

If a Personal Data breach has occurred at an IIJ Business Entity, each IIJ Business Entity's Chief Privacy Office and IIJ Business Entity's CPO shall, in cooperation with the IIJ Chief Privacy Office, IIJ CPO and the DPO, promptly notify the Commissioner to that effect, including the provision of documentation upon request (including the facts relating to the breach, its effects and the remedial actions taken). In order to ensure necessary notification to the relevant parties, the IIJ Business Entities shall follow the procedures in Section 2.6.2.

9. Tools of Accountability and Data Protection for Projects (Data Protection by Design)

9.1. Data Protection Impact Assessment

IIJ Business Entities shall determine the necessity of and shall carry out data protection impact assessments for processing operations that are likely to result in a high risk to the rights and freedom of natural persons. If the results show that the processing would result in high risk in the absence of measures taken by IIJ Business Entities to mitigate the risks, the IIJ Business Entities shall consult the Commissioner, prior to processing.

9.2. Data Protection by Design and by Default

IIJ Business Entities, acting as Data Controller, shall implement appropriate technical and organizational measures which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to facilitate compliance with the IIJ UK BCR-C. In particular, IIJ Business Entities undertake to implement technical and organisational measures ensuring that the amount and nature of Personal Data collected, the extent of processing, the period of their storage and their accessibility are necessary for each specific purpose of the processing.

9.3. Development of Products and Services

When an IIJ Business Entity develops new products or services that entail the processing of Personal Data, as of the beginning of these projects, it shall take into account and implement appropriate technical and organisational security measures.

For this objective, the project teams in charge will carry out identification of Personal Data and risk analysis in accordance with the procedures of Annex 2 “Scope of Personal Data - Procedures for Identifying Personal Data” and Annex 3 “Procedures Regarding Risk Analyses, etc. Relating to Personal Data,” and shall report those results to the relevant IIJ Business Entity’s Chief Privacy Office. The IIJ Business Entity’s Chief Privacy Office that has received the above report will confirm the results of the risk analysis, and make relevant recommendations as well as offer necessary support regarding the processing of Personal Data.

9.4. Development of New Business and Mergers & Acquisitions

Where an IIJ Business Entity intends to develop new business or to merge with or acquire

a company, as of the beginning of these projects, it shall take into account and implement appropriate technical and organisational measures.

For this purpose, the relevant IIJ Business Entity's Chief Privacy Office shall be involved as of the beginning of the project and at every stage of the project, as necessary, and make recommendations to make sure all data protection aspects are taken into account.
Where the IIJ Business Entity's Chief Privacy Office considers it necessary, it can seek the support of the IIJ Chief Privacy Office.

10. Notification to the Commissioner

Where the Commissioner requests prior notification of processing, the IIJ Business Entity shall comply with such requirements.

Where an IIJ Business Entity acts as a Data Controller, its Chief Privacy Office shall keep records of processing activities which are implemented by the IIJ Business Entity and will gather all prior notification applications that are submitted to the Commissioner.

11. Training and Improving Awareness

IIJ Business Entities will provide the following training and awareness improvement programme for Executives and Others, subject to the instruction of the DPO:

- basic information security training for the Executives and Others of the IIJ Business Entities. Such training shall be adapted to take account of local special characteristics as necessary;
- they shall provide individual and specific training as necessary for employees who participate in the development of tools to use in the collection or in the processing of Personal Data or who have periodic or permanent access to Personal Data.

Personnel responsible for education on Personal Data protection (hereinafter referred to as "Persons in charge of Training" or "Training Managers") will be appointed by the IIJ Business Entity's CPO.

Education on Personal Data protection shall include at least the following items.

1) The importance of conformity with laws and ordinances concerning Personal Data protection and its advantages;
2) The division of roles and responsibilities within the company to comply with laws and regulations concerning the protection of Personal Data; and
3) The expected results upon violation of laws relating to Personal Data protection.

The Training Managers shall formulate an "annual training plan" every fiscal year and obtain the IIJ's Business Entity's CPO's approval. The Training Managers shall create individual training plans for the training on Personal Data protection on the basis of the "annual training plan" and implement training programme according thereto, and report the results of the implementation to the IIJ Chief Privacy Office.

All Executives and Others will be required to attend these trainings and awareness improvement sessions as part of their induction program and at least once every year. The effectiveness of the IIJ UK BCR-C is maintained and improved by creating an annual training plan, and providing information security training sessions for new employees and at least once a year. Executives and Others cannot process and transfer Personal Data if they are not up to date with their training schedule.

The Training Managers will create and keep a record of trainings, and will report to the

IIJ Business Entity's CPO and IIJ CPO according to the instruction of the DPO once or every business year. The Training Managers shall record the Executives and Others who participated in the trainings and those who did not participate, and set re-education opportunities for those who did not participate.

The level of understanding is checked among the Executives and Others at the end of the trainings, in order to ensure an appropriate degree of understanding and application of the IIJ UK BCR-C and data protection laws. Participants' understanding is checked by questions on the content of the training sessions; based on their answers, those whose depth of understanding is gauged to be above a certain level from their answers are exempt from participation in a supplemental training program.

The Training Managers shall review and report the effects of the training/education, which should be reflected in the "annual training plan". The Training Managers shall also prepare once a year a report for the IIJ Business Entity's CPO and IIJ CPO, regarding the content and implementation of the results of the training program.

12. Audits

The compliance of the IIJ Business Entities with the IIJ UK BCR-C is verified through periodic audits or on the specific request of the IIJ CPO, an IIJ Business Entity's CPO or the DPO. IIJ Business Entities may also be subject to audit upon request of the Commissioner, pursuant to Section 8.2. All IIJ Business Entities are obliged to subject themselves to such audits of compliance with the IIJ UK BCR-C. Audits take place at least once every year, and cover all aspects of this BCR Policy, including methods of ensuring that corrective actions will be taken.

Each IIJ Business Entity's Internal Audit Office in cooperation with the DPO conducts such audits based on the "Basic Audit Plans" which it draws up annually. The President shall appoint those who understand the rules concerning Personal Data protection and the contents of domestic laws and regulations, and who are in a fair and objective position, as the personnel of the Internal Audit Offices responsible for Personal Data protection audits ("**Personal Data Protection Auditors**").

The Personal Data Protection Auditors shall be responsible for regularly evaluating and confirming at least the following matters:

- Compliance with the IIJ UK BCR-C, the UK GDPR and local laws;
- Management of IT systems, applications, and data bases processing Personal Data;
- Contracts affecting the implementation of this BCR Policy;
- Transfers of Personal Data outside the IIJ Business Entities (in their capacities as either Data Controllers or Data Processers);
- Implementation of corrective measures responding to issues identified as a result of internal audits.

The Personal Data Protection Auditors appoint auditors from within the company to conduct audits under their supervision.

In principle, such audits will be conducted on-site and will cover all aspects of compliance with the IIJ UK BCR-C Policy. If necessary, paper-based audits can also take place.

Personal Data Protection Auditors and persons responsible for the audits shall conduct audits as specified below.

1) Prepare a "Basic Audit Plan" for each fiscal year and obtain approval of the IIJ

Business Entity's CPO.

2) Prepare "Audit Individual Plans" based on the Basic Audit Plan.
3) Perform audits according to the Audit Individual Plans, prepare "Audit Reports" and report the results of the audits to the IIJ Business Entity's CPO and the IIJ Business Entity's Chief Privacy Office.
4) Matters to be improved which are identified as a result of the audits shall be stated in the Audit Reports where needed and recommendations for improvement shall be given to the persons responsible for data protection matters in the relevant departments of the IIJ Business Entity.
5) The person(s) responsible for data protection matters in a given department in each IIJ Business Entity and who is responsible for the employees in his/her department that process Personal Data, shall identify the underlying causes of any non-compliance identified in the course of audits and create a proposal for a corrective and preventive action plan to address the non-conformities, on the basis of which plan measures shall be taken. The corrective and preventive action plan shall be approved by the IIJ Business Entity's CPO.
6) The Personal Data Protection Auditor shall follow up on improvement activities and report the status of corrections and improvements to the IIJ Business Entity's CPO on a timely basis.

Personal Data Protection Auditors and auditors cannot conduct audits of departments to which they belong. Such audits shall be conducted separately by persons nominated by IIJ Business Entity's CPO. Any such audit shall be subject to the provisions of the preceding paragraph, *mutatis mutandis*.

The IIJ Business Entity's CPO and the persons responsible for data protection matters in the IIJ Business Entity's departments, shall report the implementation results of the audits to the IIJ Chief Privacy Office at least once a year. IIJ Chief Privacy Office shall collate the details of the reports received, and reports the contents to the IIJ CPO, who in turn informs the DPO, the President of IIJ and the board of directors of IIJ.

If the audit report reveals risks that should be shared among IIJ Business Entities or that constitute significant or new information, the report is submitted by email or in person to the IIJ Chief Privacy Office and the board of directors of IIJ. The IIJ Chief Privacy Office will consider the necessity of disseminating the information to all IIJ Business Entities and whether any further corrective actions should be undertaken.

Furthermore, IIJ Business Entities will provide, upon request and without restrictions, copies of any audit reports to the Commissioner and provide the Commissioner with power to carry out a data protection audit of any IIJ Business Entity if required, and without restrictions.

13. System to Promote BCRs

13.1 General system

IIJ, the ultimate parent company of the IIJ Group, has an IIJ CPO and IIJ Chief Privacy Office. Furthermore, each IIJ Business Entity has an IIJ Business Entity's CPO and IIJ Business Entity's Chief Privacy Office, a security control department in charge of ensuring the protection of Personal Data, as well as supervising security control in IIJ Business Entities.

The President of each IIJ Business Entity shall appoint the IIJ Business Entity's CPO as the person responsible for Personal Data protection in the IIJ Business Entity, and to undertake the duties and roles relating to Personal Data protection on a local level, such as monitoring training and compliance, overseeing the handling of local complaints and inquiries from Data Subjects, reporting major privacy issues to the DPO, etc.

The IIJ CPO and each IIJ Business Entity's CPO will consult with the DPO whenever they face a question regarding the interpretation or application of the data protection laws that has not been resolved by reference to the existing rules and guidance.

For more details on the organisational system to promote the IIJ UK BCR-C in IIJ Business Entities, refer to Annex 6 "Rules Regarding the Personal Data Protection Organization."

13.2 DPO

The President of IIJ designates the DPO which has a responsibility to monitor compliance with the IIJ UK BCR-C. The President of IIJ shall ensure that the DPO does not receive any instructions regarding the exercise of their tasks and that the DPO is involved properly and in a timely manner in all issues which relating to their respective tasks, and shall support the DPO in performing their respective tasks.

The DPO reports directly to the President of IIJ, and can be assisted by the staffs, such as IIJ CPO, IIJ Chief Privacy Office, IIJ Business Entity's CPO and IIJ Business Entity's Chief Privacy Office.

The DPO shall perform the following tasks:

- Provide advice and oversight to the IIJ Business Entities and the employees who carry out processing of their obligations pursuant to the UK Data Protection Law and

other applicable data protection laws in Third Countries, including, where requested, with respect to handling Data Subject complaints and preparing responses to exercises of rights by Data Subjects, assessing security incidents or Personal Data breaches and possible related regulatory obligations, etc.;

- Investigate, monitor and annually report on IIJ Business Entities' compliance at a global level with respect to the UK Data Protection Law and other applicable data protection laws in Third Countries, and IIJ's related data protection policies (including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits); and report the results to the board of directors;
- Provide advice where requested as regards the data protection impact assessments and monitor performance under Article 35 of the UK GDPR;
- Cooperate with the Commissioner;
- Act as a contact point for the Commissioner on any issues relating to data processing, including prior consultation under Article 36 of the UK GDPR, and consult, where appropriate, with regard to any other matter.

14. Key Performance Indicators (KPI)

In order to ensure an effective implementation of this BCR Policy, the IIJ Chief Privacy Office shall maintain the KPIs below. Each IIJ Business Entity's Chief Privacy Office shall at least once a year report the following KPIs to the IIJ Chief Privacy Office, without being limited to them:

- Number of complaints received by employees
- Number of requests for access to one's Personal Data
- Number of data breaches
- Number of notifications to the Commissioner
- Number of SCCs (Standard Contractual Clauses) concluded for transfers of Personal Data

15. Investigations

In case of investigation requests from the Commissioner, the relevant IIJ Business Entity's Chief Privacy Office shall promptly contact the IIJ Chief Privacy Office.

As it is stipulated in Section 8 "Cooperation Mechanism," the IIJ Business Entity's Chief Privacy Office and the IIJ Chief Privacy Office shall actively cooperate in order to respond to requests from the Commissioner regarding investigations.

16. Control of Documents and Records

16.1. Update of the IIJ UK BCR-C Policy

This BCR Policy may be amended from time to time and as necessary, in order to reflect changes in the UK Data Protection Law, to factor in modifications of the regulatory environment or company structure, etc., provided that any such amendments do not undermine any protections afforded to Data Subjects. All such modifications will be reported without undue delay to the Commissioner and to all IIJ Business Entities, as set forth below.

IIJ shall be responsible for promptly informing the Commissioner and IIJ Business Entities of any substantial, critical or material changes to this IIJ UK BCR-C Policy, including those which potentially affect data protection compliance, are potentially detrimental to Data Subject rights, potentially affect the level of protection offered by the BCR Policy, affect the binding nature of the BCR Policy, etc.

Administrative revisions to the IIJ UK BCR-C Policy, including updates to the list of IIJ Business Entities bound by this BCR Policy, shall be reported without undue delay to all IIJ Business Entities as well as to the Commissioner. Any revisions to this BCR Policy and to the list of IIJ Business Entities bound by this BCR Policy shall be reported to the Commissioner at least once a year with a brief explanation of the reasons justifying the update.

In the event that a new entity becomes a member of the IIJ Group with the intention that the entity will be involved in processing Personal Data from the UK, it may accede to the Intra-Group Agreement in accordance with the provisions of that Agreement. No transfers of Personal Data will occur to new IIJ Group members until such time as they are effectively bound by and can deliver compliance with this BCR Policy, or until another mechanism is in place to secure the transfer in accordance with the UK GDPR (e.g. standard contractual clauses).

IIJ will also be responsible for providing the Commissioner with relevant materials and information in order to assist it in understanding the details of, including justifications for, the revisions.

The IIJ CPO in cooperation with the DPO shall keep a fully updated list of the IIJ Business Entities, shall keep track of and record any updates to the rules, and shall provide the

necessary information to the Data Subjects and the Commissioner upon request.

16.2. Records of Processing Activities

Each IIJ Business Entity's Chief Privacy Office shall maintain a record of processing activities carried out by it either as Data Controller or as Data Processor. That record shall contain all of the following information:

- the name and contact details of the Data Controller and, where applicable, the joint Data Controller, the Data Controller's representative and the DPO;
- the purposes of the processing;
- a description of the categories of Data Subjects and of the categories of Personal Data;
- the categories of recipients to whom the Personal Data have been or will be disclosed, including recipients in Third Countries or international organisations;
- where applicable, Personal Data Transfers to a Third Country or an international organisation, including the identification of that Third Country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the UK GDPR, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security protection measures referred to in Article 32(1) of the UK GDPR or, as appropriate, the security measures referred to in section 28(3) of the Data Protection Act 2018.

This record should be maintained in writing, including in electronic form, and should be made available to the Commissioner on request.

17. RACI

Refer to Annex 7 “RACI” for the roles and responsibilities regarding the IIJ UK BCR-C.

18. Annexes

Annex 1 “Definitions of IIJ Business Entities”
Annex 2 “Scope of Personal Data - Procedures for Identifying Personal Data”
Annex 3 “Procedures Regarding Risk Analyses, etc. Regarding Personal Data”
Annex 4 “Rules Regarding the Data Subject’s Personal Data Rights”
Annex 5 “Procedures Regarding Complaints and Consultations Relating to Personal Data”
Annex 6 “Rules Regarding the Personal Data Protection Organization”
Annex 7 “RACI”
Annex 8 “Rules Regarding the Training on Personal Data Protection”
Annex 9 “Rules Regarding Audits related to Personal Data Protection”

19. Revisions and Discontinuation

Revisions or abolishment of the IIJ UK BCR-C will be carried out with the approval of the IIJ CPO.

END

Supplementary Provisions

The IIJ UK BCR-C Policy is enacted from 14th March 2025.