IIJ UK BCR-P

（Processor 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 Processor or Sub-Processor, IIJ has adopted these Binding Corporate Rules (the "**IIJ UK BCR-P**" or these "**BCRs**").

1.2. Scope

1.2.1. Geographic Scope

The IIJ UK BCR-P apply to the processing of 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 within the United Kingdom (the "**UK**") by a Data Controller to IIJ Business Entities acting as a Data Processor or Sub-Processor outside the UK, regardless of the nature of the Personal Data being processed. Specifically, the IIJ UK BCR-P applies to the Personal Data provided to the IIJ Business Entities by:

(i) Data Controllers in the UK which shall process Personal Data in accordance with the UK GDPR; or

(ii) Data Controllers outside the UK which shall process Personal Data in accordance with the UK GDPR due to its exterritorial application or for other reasons, including the conclusion of standard contractual clauses.

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

Where an IIJ Business Entity acts as a Data Processor on behalf of a Data Controller, it shall be the sole responsibility of that Data Controller to determine whether these BCRs

shall apply to Personal Data processed by the IIJ Business Entity on behalf of such Data Controller (i) only to the extent such Personal Data are subject to UK law (e.g., only to Personal Data transferred from the UK), or (ii) regardless of the origin of such Personal Data.

Where an IIJ Business Entity acts as a Data Processor on behalf of another IIJ Business Entity acting as a Data Controller, these BCRs shall apply to all Personal Data processed by the IIJ Business Entity on behalf of such Data Controller, regardless of the origin of such Personal Data.

1.2.2. Standing vis-à-vis IIJ Business Entities

The IIJ UK BCR-P 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-P Policy. The IIJ Business Entities, including their employees, must also respect the instructions from the Data Controller regarding the data processing and the security and confidentiality measures as provided in the Service Agreement.

1.2.3. Standing vis-à-vis Employees

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

1.4. Related Documents

The IIJ UK BCR-P Policy also comprises the Annexes listed in Section 18 which describe the procedures that guarantee the effective implementation of the IIJ UK BCR-P 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-P Policy, Data Controller refers to an external (non-IIJ) entity.
Data Processor	Natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller and subject to the terms of a Service Agreement therewith. For purposes of the IIJ UK BCR-P 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-P and data protection laws at a global level. If any events relevant to compliance with the IIJ UK BCR-P 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.

Term	Definition
IIJ Business Entities or IIJ Business Entity	Companies to which the IIJ UK BCR-P 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 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-P 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

Term	Definition
	and operation of the IIJ UK BCR-P for the IIJ Business Entities; supervising the overall implementation of the IIJ UK BCR-P 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 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-P 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 Processor for transfers or a set of transfers of Personal Data to a Data Processor in one or more Third Countries. The IIJ UK BCR-P Policy and the Intra-Group Agreement that makes the Policy biding upon the IIJ Business Entities constitute the IIJ UK BCR-P.
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,

Term	Definition
	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-P 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.
Service Agreement	The binding agreement between the IIJ Business Entity acting as Data Processor and the Data Controller, which agreement complies with Article 28 of the UK GDPR.
Sub-Processor	Natural or legal person, public authority, agency or other body directly engaged by an IIJ Business Entity acting as Data Processor or Sub-Processor, with the authorization of the Data Controller (pursuant to Section 2.2 herein) to assist in fulfilling the Data Processor's obligations set forth in the Service Agreement (to which agreement the Sub-Processor is generally not party). For purposes of the IIJ UK BCR-P Policy, Sub-Processor refers to one of the IIJ Business Entities or an external entity.
Third Country or Third Countries	Any country or territory outside the UK.
Third Party	Natural or legal person, Public Authority or Public Body, excluding the Data Subject, the Data Controller, any IIJ Business Entity, 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-P, excluding the person who is defined as

Term	Definition
	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-P 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-P Policy. Where there are aspects of the IIJ UK BCR-P Policy that are subject to more stringent local legislation, the more stringent legislation will apply to these aspects.

Data Processors and Sub-Processors. Any IIJ Business Entity acting as a Data Processor (or Sub-Processor), in addition to complying with the IIJ UK BCR-P, shall comply with the data processing procedures and security measures agreed to with the Data Controller. The IIJ Business Entity acting as a Data Processor or Sub-Processor (including any Executives and Others of such IIJ Business Entity) has a duty to respect the instructions of the Data Controller for processing, security and confidentiality, as well as for Personal Data Transfers to Third Countries. If, for any reason, the IIJ Business Entity (or any Executives and Others of the IIJ Business Entity) determines that it cannot follow the procedures prescribed by and instructions from the Data Controller, it shall promptly notify the Data Controller.

Relationship between National Law and the IIJ UK BCR-P Policy. If an IIJ Business Entity as a Data Processor, 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-P Policy or Service Agreement or the instructions from the Data Controller, or would have a substantial effect on the guarantees provided by the IJ UK BCR-P Policy, the person in charge of such IIJ Business Entity shall promptly inform the Data Controller (which is entitled to suspend the transfer of data and/or terminate the contract) and the IIJ Lead Business Entity of the issue, and seek support from the 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-P Policy and local laws, and where these conflicts cannot be quickly dispelled and/or resolved, the IIJ Business Entity's Chief Privacy Office will correspond with the Commissioner as to the matter.

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-P Policy (including legally binding requests for disclosure of Personal Data by a law enforcement authority or state security body), the

IIJ Business Entity shall suspend the request and promptly and clearly inform the Commissioner and the Data Controller unless otherwise prohibited from doing so (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). The IIJ Business Entity shall provide the Commissioner with 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. In this regard, the IIJ Business Entity's CPO shall cooperate with the DPO to inform the Commissioner and, where required, the Data Controller.

If in specific cases the suspension and/or notification are prohibited, the IIJ Business Entity will use its best efforts to obtain the right to waive such prohibition and 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 on the requests it receives at least once a year (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 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

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

2.2. General Principles Relating to Processing of Personal Data

The IIJ Business Entity as a Data Processor will comply with the general principles set forth in this Section 2 by (i) complying with the instructions of the Data Controller with respect to the processing of Personal Data, and (ii) upon request of the Data Controller, providing such further cooperation and assistance as reasonably required by the Data Controller to comply with its own obligations, in a reasonable time, in any case, without undue delay, and to the extent reasonably possible. If the IIJ Business Entity finds itself in a position where it cannot comply with the general principles referred to above, it shall promptly notify the Data Controller to that effect.

In particular, to give effect to the foregoing, the IIJ Business Entity acting as a Data Processor or Sub-Processor shall observe the following principles:

i. **Transparency, Fairness and Lawfulness**: Data Processors and Sub-Processors have a general duty to help and assist the Data Controller to comply with the law and to demonstrate such compliance (such as for answering Data Subject requests in relation to their rights, by being transparent about Sub-Processor activities in order to allow the Data Controller to correctly inform Data Subjects, etc.). This includes the obligation to make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's or Sub-Processor's obligations pursuant to Article 28(3)(h) of the UK GDPR, and to allow for and contribute to audits, including inspections conducted by the Data Controller or another auditor mandated by the Data Controller. In addition, the Data Processor or Sub-Processor must immediately inform the Data Controller if, in its opinion, an instruction infringes any provision of the UK Data Protection Law.

ii. **Purpose Limitation**: Data Processors and Sub-Processors have a duty to process Personal Data only on behalf of the Data Controller and in compliance with its documented instructions, including as regards transfers of Personal Data to a Third Country or international organisation. In the event that UK domestic law prevents the Data Processor from processing in accordance with the Data Controller's documented instructions, the Data Processor shall inform the Data Controller of that legal requirement before any processing takes place, unless such disclosure is prohibited on important grounds of public interest (in accordance with Article 28(3)(a) of the UK GDPR). In all other cases, if the Data Processor cannot provide

the above-stipulated compliance for whatever reasons, it shall promptly inform the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the transfer of Personal Data and/or terminate the contract. Each IIJ Business Entity listed in Annex 1 acting as Data Processor, and their Executives and Others who are involved in the processing activities, shall respect and comply with the instructions from the Data Controller regarding the processing and security and confidentiality measures applicable to the Personal Data;

iii. **Data Quality**: Data Processors and Sub-Processors have a general duty to help and assist the Data Controller to comply with the law, in particular by executing any necessary measures upon the request of the Data Controller (and in accordance with the terms of the Service Agreement) in order to delete, update or rectify the Personal Data, or to have the Personal Data deleted or anonymized from the moment the identification form is no longer necessary, as well as to notify other IIJ Business Entities or any external Sub-Processors to which the Personal Data has been disclosed of such request, so that they can also update their records accordingly;

iv. **Security and Data Breaches**: Data Processors and Sub-Processors have the following security-related duties:

- Duty to implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by processing, which at least meet the requirements of Article 32 of the UK GDPR and any existing specific measures specified in the Service Agreement;
- Duty to assist the Data Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the UK GDPR, taking into account the nature of the processing and the information available to the Data Processor (or Sub-Processor);
- After becoming aware of any Personal Data breach, duty for Data Processors to inform the Data Controller without undue delay or in the case of Sub-Processors, to inform the Data Processor and the Data Controller without undue delay.

v. **Data Subject Rights**: Data Processors and Sub-Processors must execute any appropriate technical and organizational measures insofar as this is possible, when asked by the Data Controller, and communicate any useful information in order to assist the Data Controller for the fulfilment of the Data Controller's obligations to respond to requests for exercising the Data Subjects rights as set out in Chapter III of the UK GDPR, and including by communicating any useful information in order to help the Data Controller to comply with its duty to respect the rights of the Data

Subject. The Data Processor and Sub-Processors shall transmit without delay requests received from Data Subjects to the Data Controller without answering such requests, unless authorized by the Data Controller to do so;

vi. **Sub-Processing within the Group and to external entities**: IIJ Business Entities may arrange the sub-processing of Personal Data by other IIJ Business Entities or by external entities only with the prior informed specific or general written authorisation of the Data Controller, including the disclosure to the Data Controller of information regarding the main elements of such proposed sub-processing arrangement (i.e. the parties, countries, security, guarantees in case of international transfers, and possibility to receive a copy of the contacts used).

- Whether the Data Controller's general written authorisation is sufficient, or a specific authorisation for each new Sub-Processor is required, shall be set forth in the Service Agreement. If a general authorization is given, the Data Controller should be informed by the Data Processor of any intended changes concerning the addition or replacement of Sub-Processors in such a timely fashion that the Data Controller has the possibility to object to the change or to terminate the contract before the data are communicated to the new Sub-Processor.
- In the event that an IIJ Business Entity as Data Processor subcontracts its obligations under the Service Agreement, with the authorisation of the Data Controller, such IIJ Business Entity shall do so only by way of contract or other legal act under UK law with the Sub-Processor. Such contract or other legal act shall (1) provide that adequate protection is provided as set out in Articles 28, 29, 32, 45, 46 and 47 of the UK GDPR and (2) ensure that the same data protection obligations as set out in the Service Agreement between the Data Controller and the IIJ Business Entity and also in the IIJ UK BCR-P Policy (including but not limited to this Section 2.2) are imposed on the Sub-Processor. It shall, in particular, provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the UK GDPR. For example:
  - The Sub-Processor must not process the Personal Data except on instructions from the IIJ Business Entity, unless the Sub-Processor is required to do so by law.
  - The Sub-Processor must implement appropriate technical and organizational measures to protect Personal Data against accidental

or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the Personal Data to be protected.

- The Sub-Processor must comply with Section 3.5 herein prior to effecting any transfer of Personal Data outside the UK;
- The Sub-Processor must accept that its facilities may be audited by the Data Controller at the Data Controller's request, or by an inspection body selected by the Data Controller and composed of independent members with the required professional qualifications, bound by a duty of confidentiality; and
- The Sub-Processor may only engage another Sub-Processor pursuant to the same obligations set forth above and pursuant to these BCRs.

vii. **Termination**: The Data Processor must promptly inform the Data Controller of any inability to process Personal Data on its behalf and to comply with its instructions, including where the Data Processor has reason to believe that existing or future local legislation in Third Countries applicable to it may prevent it from fulfilling the instructions received from the Data Controller or other obligations under these BCRs, in which case the Data Controller will be entitled to suspend the transfer of Personal Data and/or terminate the contract. If the contract and provision of data processing services by the Data Processor is cancelled or otherwise terminated in the manners set forth above or otherwise, the IIJ Business Entity will, at the choice and in accordance with the instructions of the Data Controller, delete or return all the Personal Data to the Data Controller and delete all copies thereof, and certify to the Data Controller that it has done so, unless applicable local legislation in Third Countries imposed upon the IIJ Business Entity requires storage of the Personal Data transferred. In such case, the IIJ Business Entity will inform the Data Controller thereof and warrant that it will guarantee the confidentiality of, and will no longer actively process, the Personal Data transferred.

2.3. Collection of Personal Data

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

2.4. Processing the Personal Data of Children

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

2.5. Processing Sensitive Data

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

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.

In addition, where an IIJ Business Entity is acting as the Data Processor, it shall:

- cooperate with and assist the Data Controller without undue delay and to the extent reasonably possible in complying with its obligations under the UK Data Protection Law and the BCR Policy;
- comply with the requirements of the Data Controller regarding the appointment of any Sub-Processor. The IIJ Business Entity will also ensure that Sub-Processors undertake to comply with provisions which are consistent with (i) the terms of the Service Agreement with the Data Controller and (ii) the IIJ UK BCR-P Policy, and in particular that the Sub-Processor will adopt appropriate and equivalent security measures;
- put in place appropriate technical and organisational measures to safeguard Personal Data processed on behalf of the Data Controller, including by complying with the security requirements prescribed by the Data Controller; and
- notify the Data Controller of any security breach, in accordance with the terms of the

Service Agreement with that Data Controller and as set forth below.

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'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.

Any IIJ Business Entity as a Data Processor shall have a duty to inform the Data Controller without undue delay after becoming aware of any Personal Data breach. In addition, the IIJ Business Entity as a sub-Processor shall have a duty to inform both the Data Processor and the Data Controller without undue delay after becoming aware of any Personal Data breach.

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 transfer Personal Data of customers (and their customers), suppliers and service providers to and between the IIJ Business Entities or external sub-Processors engaged by IIJ Business Entities, both within and outside of the UK. For the avoidance of doubt, transfer of Personal Data to external sub-Processors outside of the UK may be conducted only where the conditions laid down in Article 45, 46 or 49 of the UK GDPR are complied with by the relevant IIJ Business Entities and external sub-Processors.

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

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: Case 1: (1) Case manager of IIJ Business Entity receives customer data from customer by means specified by the customer, (2) Case manager of IIJ Business Entity browses customer data and processes that Personal Data, according to the procedure specified by customer.

  Case 2: (1) Client sends customer data on cloud service (SaaS) provided by IIJ Business Entity and processing of data sent on service is performed, (2) The case manager of IIJ Business Entity does not have access to the data stored by the customer normally, but access may be granted to him/her when the customer requests support, and as part of the support requested by the customer he/she may view and process customer data.

  Case 3: (1) Customer builds their own system environment on cloud service (PaaS / IaaS) provided by IIJ Business Entity, and customer stores customer data on the environment, (2) The case manager of IIJ Business Entity does not have the right to access the system which the customer has built independently, and does not perform maintenance, he/she does not browse and process customer data.
- 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.

IIJ's customers' 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 customers of IIJ Business Entities
- Types of processing:

  Case 1: (1) Case manager of IIJ Business Entity receives customer data from customer by means specified by the customer, (2) Case manager of IIJ Business Entity browses customer data and processes that Personal Data, according to the procedure specified by the customer.

  Case 2: (1) Client sends customer data on cloud service (SaaS) provided by IIJ Business Entity and processing of data sent on service is performed, (2) The case manager of IIJ Business Entity does not have access to the data stored by the customer normally, but access may be granted to him/her when the customer requests support, and as part of the support requested by the customer he/she may view and process customer data.

  Case 3: (1) Customer builds their own system environment on cloud service (PaaS / IaaS) provided by IIJ Business Entity, and customer stores customer data on the environment, (2) The case manager of IIJ Business Entity does not have the right to access the system which the customer has built independently, and does not perform maintenance, he/she does not browse and process customer data.
- Countries to which IIJ's customers' customer 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.

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 from the UK 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.

In order 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 transfers of such Personal Data to, from and between the IIJ Business Entities located within or outside 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

[Section intentionally blank in IIJ UK BCR-P]

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

[Section intentionally blank in IIJ UK BCR-P]

3.3. Personal Data Transfer from Data Controller to an IIJ Business Entity located within the UK

Where an IIJ Business Entity as a Data Processor that is located within the UK receives Personal Data to which the UK GDPR applies from a Data Controller, that IIJ Business Entity as Data Processor shall enter into a Service Agreement with the Data Controller, and the IIJ UK BCR-P shall be made binding toward the Data Controller.

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 Outside the UK

Where an IIJ Business Entity, acting as a Data Processor, transfers Personal Data to which the UK GDPR applies to another IIJ Business Entity (acting as Sub-Processor) located outside the UK, the Personal Data Transfer is covered by this BCR Policy. In such event, the IIJ Business Entity as Data Processor must also enter into a written agreement that at minimum meets the requirements of Articles 28(3) and 28(4) of the UK GDPR, with such IIJ Business Entity acting as Sub-Processor (unless the IIJ Business Entity acting as Sub-Processor is party to the Service Agreement between the IIJ Business Entity acting as Data Processor and the Data Controller).

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

Where an IIJ Business Entity acting as a Data Processor subcontracts its obligations under the Service Agreement to an external Sub-Processor (with the authorization of the Data Controller and subject to the provisions set forth in Section 2.2), the IIJ Business Entity transferring the Personal Data shall ensure that the external Sub-Processor receiving the Personal Data commits in writing, by way of a contract or other legal act under UK law, to providing sufficient guarantees to (i) ensure the same data protection obligations as set forth in the Service Agreement between the Data Controller and the Data Processor, including by implementing appropriate technical, security, confidentiality and organisational measures in such a manner that the processing of the Personal Data will meet the requirements of the Articles 28(3) and 28(4) of the UK GDPR; and (ii) obligate the contracting Sub-Processor to provide adequate protection for the Personal Data as set forth under Articles 28, 29, 32, 45, 46 and 49 of the UK GDPR. For the avoidance of doubt, this shall include the obligation not to conduct any transfer of Personal Data unless such transfer of Personal Data is conducted in compliance with the UK Data Protection Law, in particular:

i. reliance on adequacy regulations under section 17A of the Data Protection Act 2018 (according to Article 45 of the UK GDPR),
ii. execution of appropriate standard data protection clauses as 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. implementation of another appropriate safeguard pursuant to Article 46 of the UK GDPR, or

iv. reliance on a derogation according to Article 49 of the UK GDPR.

4. Rights of Data Subject

4.1. Right of Access by the Data Subject

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

4.2. Right to Rectification

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

4.3. Right to Erasure (Right to be Forgotten)

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

4.4. Right to Restriction of Processing

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

4.5 Right to Data Portability

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

4.6 Right to Object

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

4.7 Automated Individual Decisions

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

4.8 Right to Withdraw Consent

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

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

All Data Subjects have the right to have easy access to the IIJ UK BCR-P Policy, which right requires that all Data Subjects benefiting from Third Party Beneficiary rights be

provided with all the information pertaining to their Third Party Beneficiary rights relating to the processing of their Personal Data and to the means to exercise those rights. For this reason, the IIJ UK BCR-P 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-P Policy will also be made available on the intranet.

4.10. Handling a Request from a Data Subject

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

5. Complaint Handling Procedures

5.1. Direct Complaints

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

5.2. Indirect Complaints

If any Data Subject has filed a complaint against the processing of his/her Personal Data by an IIJ Business Entity acting as a Data Processor, that IIJ Business Entity will actively support the complaint handling process that the Data Controller carries out.
Data Subjects may submit complaints by sending an email to the following address.
iijgroup-dpo-contact@iij.ad.jp.

Further, the IIJ Business Entity shall have the duty to communicate a claim, request or complaint without undue delay to the Data Controller, without obligation to handle it (except if it has been agreed otherwise with that Data Controller).

Where an IIJ Business Entity acts as a Data Processor, and where the Data Controller on whose behalf it processes the Personal Data factually disappears, ceases to exist in law or has become insolvent, the IIJ Business Entity will undertake to handle the complaint in accordance with the procedures stipulated in Annex 5, "Procedures Regarding Complaints and Consultations Relating to Personal Data", which sets forth the practical steps of the IIJ complaint system. In all cases where the IIJ Business Entity as a Data Processor handles complaints, these shall be dealt without undue delay and in any event within one (1) month by the IIJ Business Entity's CPO. Taking into account the complexity and number of the requests, the time frame for response can be extended by two (2) further months at most. In such case, the Data Subject should be informed

accordingly.

Data Subjects may also submit a complaint or claim with the Commissioner or before a court or other competent authority in the UK, without first exhausting the IIJ Group's or Data Controller's complaint process.

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-P as Third Party Beneficiaries directly against the IIJ Business Entity as Data Processor in the event of a breach by any IIJ Business Entity of *any* of its commitments herein, including but not limited to:

- Purpose limitation (Section 2.2 of the IIJ UK BCR-P Policy),
- Data quality and proportionality (Section 2.2 of the IIJ UK BCR-P Policy),
- Transparency and easy access to BCRs (Sections 2.2 and 4.6 of the IIJ UK BCR-P Policy),
- Security and confidentiality including data breach notifications (Section 2.6 of the IIJ UK BCR-P Policy),
- Restrictions on onward transfers, including to external entities outside of the IIJ Group (Sections 2.2 and 3 of the IIJ UK BCR-P Policy),
- National legislation preventing respect of BCRs (Section 2 of the IIJ UK BCR-P Policy),
- Right to complain through the internal complaint mechanism of the BCRs members (Section 5.2 of the IIJ UK BCR-P Policy),
- Cooperation with the Data Controller including the duty to respect instructions (Sections 8.1 and 16.2 of the IIJ UK BCR-P Policy)
- Cooperation duties with the Commissioner (Section 8.2 of the IIJ UK BCR-P Policy),
- Liability, burden of proof and jurisdiction provisions (Section 6 of the IIJ UK BCR-P Policy),
- Data protection by design and by default (Section 9.2 of the IIJ UK BCR-P Policy).

Such rights include the right to judicial remedies for any breach of this BCR Policy, including the Third Party Beneficiary rights guaranteed, and the right to obtain redress and, where appropriate, compensation for any damage (material harm including any

distress). In particular, Data Subjects are entitled to submit a complaint before the Commissioner and/or claim for judicial remedy to a competent UK court or other competent authority in the UK (see Section 180 of the Data Protection Act 2018).

In the event that a Data Subject is not able to bring a claim against the Data Controller (such as where a Data Controller on whose behalf an IIJ Business Entity processes Personal Data factually disappears, ceases to exist in law or has become insolvent - unless the legal obligations of the Data Controller vis-à-vis the Data Subject are assumed by another entity by contract or by operation of law), the Data Subject will be entitled to enforce the IIJ UK BCR-P as Third Party Beneficiaries against the IIJ Business Entity that acts as a Data Processor.

Further, where the Data Controller and the Data Processor involved in the same processing are found responsible for any damage caused by such processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from the Data Processor.

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 other non-UK IIJ Business Entities or the breaches caused by external Sub-Processors established outside of the UK, including the duty to pay compensation for any material or non-material damages resulting from the violation of this BCR Policy by such non-UK IIJ Business Entities or external Sub-Processors established outside the UK. In this regard, the IIJ Lead Business Entity shall assume ultimate liability for any such violations, as if the violations had been caused by the IIJ Lead Business Entity instead of by the IIJ Business Entity outside the UK or the external sub-Processor established outside the UK, and UK Courts or other competent authorities in the UK will have jurisdiction in such matter. Further, the IIJ Lead Business Entity shall not be entitled to rely on a breach by any IIJ Business Entity established outside the UK, or by an external Sub-Processor established outside the UK 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 or the external Sub-Processor established outside the UK is not liable for the violation, it may discharge itself from any responsibility/liability.

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

[Section intentionally blank in IIJ UK BCR-P]

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

Except as otherwise set forth in this BCR Policy, where an IIJ Business Entity is acting as a Data Processor, it shall be liable for the damage that has occurred as a result of such processing only if it has acted outside or contrary to lawful instructions of the Data Controller (including a violation of the Service Agreement therewith), or if it has breached the IIJ UK BCR-P, UK Data Protection Law or applicable data protection law in Third Countries. The Data Subjects may exercise their right to enforce the IIJ UK BCR-P to obtain an effective judicial remedy, including the right to obtain redress and to receive compensation, before a courts 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.

6.5. Burden of Proof

The IIJ Lead Business Entity will have the burden of proof to demonstrate that any IIJ Business Entity outside the UK and/or any external Sub-Processor outside the UK is not liable for any violation of the IIJ UK BCR-P which has resulted in the Data Subject claiming damages or remedy. Further, where facts can be established by the Data Controller which show that damage likely occurred because of a breach of the IIJ UK BCR-P, IIJ Lead Business Entity shall bear the burden of proof for demonstrating that the IIJ Business Entity outside the UK or the external Sub-Processor outside the UK is not responsible for the breach of the IIJ UK BCR-P giving rise to those damages or that no such breach took place. If the IIJ Lead Business Entity can prove that the IIJ Business Entity or the external Sub-Processor established outside the UK is not liable for the event giving rise to the damage, it may discharge itself from any responsibility/liability.

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

When an IIJ Business Entity acts as a Data Processor for a Data Controller, the IIJ BCR-P shall be made binding toward the Data Controller, either through an annex or via a specific electronic accessible reference to it in the Service Agreement between both entities.

Where the IIJ Business Entity, acting as a Data Processor or Sub-Processor, has failed to comply with the IIJ UK BCR-P, with the Data Controller's instructions or with the Service Agreement, the Data Controller has the right to enforce the IIJ UK BCR-P against the IIJ Lead Business Entity, as provided for in Sections 6.2 and 6.5 of the IIJ UK BCR-P Policy, including the right to receive compensation and to judicial remedy before a court or other competent authorities in the UK (see Section 180 of the Data Protection Act 2018). The Data Controller also has the right to enforce the IIJ UK BCR-P against the IIJ Lead Business Entity in case any external Sub-Processor established outside of the UK breaches the written agreement between the IIJ Business Entity acting as Data Processor and such Sub-Processor (referred to in Section 2.2(vi) of the IIJ UK BCR-P Policy).

The Data Controller shall have rights to have judicial remedies to obtain redress and compensation, as described in Section 6.2, furthermore, burden of proof applies as outlined in Section 6.5.

In any case, the IIJ Business Entity is not exempt from liability vis à vis the Data Controller, even if the violation is a result of the actions of a sub-Processor.

8. Cooperation Mechanism

8.1. Cooperation with the Data Controller

Where an IIJ Business Entity acts as a Data Processor or a Sub-Processor, it shall, within a reasonable time and to the extent reasonably possible, in any case, without undue delay, cooperate with and assist the Data Controller to comply with UK Data Protection Law as well as applicable data protection law in Third Countries, including by providing the Data Controller with information regarding its Personal Data processing activities, assisting the Data Controller with respect to Data Subject rights requests and complaints as set out in Chapter III of the UK GDPR, and responding to investigations and inquiries from the Commissioner.

Where an IIJ Business Entity acts as a Data Processor or a Sub-Processor, the IIJ Business Entity shall cooperate and comply with instructions by the Data Controller regarding the updating, correction, disposal, deletion, return or anonymization of Personal Data. Further, the IIJ Business Entity shall assist the Data Controller in ensuring compliance with the obligations concerning the security of processing, personal data breach notifications, data protection impact assessments and prior consultations (Article 32-36 of the UK GDPR).

8.2. Cooperation with the Commissioner

IIJ Business Entities shall cooperate and assist each other in order to handle requests by the Commissioner in the context of investigations, inquiries or audits.

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 therefrom. IIJ Business Entities also accept, without restrictions, to be audited by the Commissioner to verify compliance with the UK Data Protection Law, and with the IIJ UK BCR-P.

IIJ Business Entities shall make available to the Commissioner the results of verifications of compliance, which may include, but are not limited to, 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

[Section intentionally blank in IIJ UK BCR-P]

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

9.1. Data Protection Impact Assessment

[Section intentionally blank in IIJ UK BCR-P]

9.2. Data Protection by Design and by Default

IIJ Business Entities, acting as Data Processor, shall assist the Data Controller in implementing appropriate technical and organizational measures which are designed to comply with 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-P in practice, such as data protection by design and by default.

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. Notifications

Where an IIJ Business Entity acts as a Data Processor on behalf of a Data Controller, the IIJ Business Entity commits to providing the Data Controller and the Commissioner with all relevant information necessary to comply with requirements pursuant to UK domestic law and the IIJ UK BCR-P.

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 Executives and Others 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-P 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 these BCRs 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-P 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-P. 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-P, 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 Data Processers or Sub-Processors);
- 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-P 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.

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.

In addition, each IIJ Business Entity acting as a Processor or sub-Processor processing the Personal Data on behalf of a particular Data Controller shall accept, at the request of that Data Controller, to submit their data processing facilities for audit of the processing activities relating to that Data Controller which shall be carried out by the Data Controller or an inspection body composed of independent members and in possession of the required professional qualifications and bound by a duty of confidentiality, selected by the Data Controller. Where applicable, this may be in agreement with the Commissioner.

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-P 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-P. 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,

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-P 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, to all IIJ Business Entities and to the Data Controller, as set forth below.

IIJ shall be responsible for promptly informing the Commissioner, IIJ Business Entities and the Data Controller of any substantial, critical or material changes to this IIJ UK BCR-P 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-P 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, the Commissioner and the Data Controller. 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 BCRs members and Sub-Processors involved in the data processing activities on behalf of any

Data Controller, shall keep track of and record any updates, and shall provide the necessary information to the Data Controller, Data Subjects and the Commissioner upon request. The IIJ CPO in cooperation with the DPO shall additionally keep track of and record any updates to these BCRs and provide the necessary information systematically to the Data Controller and upon request, to the Commissioner.

Where a change affects the processing conditions, the information should be given to the Data Controller in such a timely fashion that the Data Controller has the possibility to object to the change or to terminate the contract before the modification is made (for instance, on any intended changes concerning the addition or replacement of sub-Processors, before the Personal Data are communicated to the new sub-Processor).

16.2. Records of Processing Activities

The IIJ Business Entities acting as Data Processor have a duty to make available to the Data Controller all information necessary to demonstrate compliance with their obligations pursuant to Article 28(3)(h) of the UK GDPR, and to allow for and contribute to audits, including inspections conducted by the Data Controller or another auditor mandated by the Controller. In addition, the Data Processor must immediately inform the Data Controller if, in its opinion, an instruction infringes the UK GDPR or Data Protection Act 2018 provisions.

In order to demonstrate compliance with these BCRs, each IIJ Business Entity's Chief Privacy Office shall maintain a record of processing activities carried out by it as Data Processor on behalf of a Data Controller, in line with the requirements set out in Article 30(2) of the UK GDPR. That record shall contain all of the following information:

- the name and contact details of the Data Processors and the Sub-Processors and of the Data Controller on behalf of which the Data Processor is acting, and, where applicable, of the Data Controller's or the Data Processor's representative and the DPO;
- the categories of processing carried out on behalf of the Data Controller;
- 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, a general description of the technical and organisational security protection measures referred to in Articles 28(3) and 32(1) of the UK GDPR.

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-P.

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” [This Annex is not contained in IIJ UK BCR-P]

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-P will be carried out with the approval of the IIJ CPO.

END

Supplementary Provisions

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