

# **IIJ BCR-P**

(Processor Policy)

Version 1.1

23rd November 2021

Internet Initiative Japan Inc.

Version No.	Revision Date	Revision Reason & Details	Approval	Creation/Revision
Ver. 1.0	28th July 2021	Initial Version	Miyoshi	Risk Management Office
Ver. 1.1	23rd November 2021	Additional note on the treatment of personal data transferred from controllers outside the EEA	Miyoshi	Risk Management Office

## Table of Contents

1. Introduction.....	6
1.1. Purpose.....	6
1.2. Scope.....	6
1.2.1. Geographic Scope.....	6
1.2.2. Standing vis-à-vis IIJ Business Entities .....	6
1.2.3. Standing vis-à-vis Employees.....	7
1.3. Document Retention and Distribution .....	7
1.4. Related Documents .....	7
1.5. Keywords.....	7
2. General Principles of Personal Data Processing .....	12
2.1. <i>Legal Basis for Personal Data Processing</i> .....	13
2.2. General Principles relating to processing of Personal Data .....	14
2.3. <i>Collection of Personal Data</i> .....	16
2.4. <i>Processing the Personal Data of Children</i> .....	16
2.5. <i>Processing Sensitive Data</i> .....	16
2.6. Security .....	16
2.7. <i>Automated Individual Decisions</i> .....	18
2.8. Procedures ensuring compliance with the Principles of Section 2 .....	18
3. Transfer of Personal Data .....	19
3.1. <i>Personal Data Transfer from an IIJ Business Entity acting as a Data Controller located within or outside the EEA to an IIJ Business Entity located within or outside the EEA</i> .....	21
3.2. <i>Personal Data Transfer from an IIJ Business Entity acting as a Data Controller, located within or outside of EEA to a Third Party located within or outside of EEA</i>	21
3.3. Personal Data Transfer from Data Controller .....	21
3.4. Personal Data Transfer from an IIJ Business Entity acting as a Data Processor .....	21
3.5. Personal Data Transfer from an IIJ Business Entity acting as a Data Processor located within or outside the EEA to a Third Party located within or outside the EEA .....	21
4. Rights of Data Subject.....	22
4.1. <i>Right of access by the Data Subject</i> .....	22
4.2. <i>Right to Rectification</i> .....	22
4.3. <i>Right to Erasure (Right to be Forgotten)</i> .....	22

4.4. <i>Right to Restriction of Processing</i> .....	22
4.5 <i>Direct Marketing</i> .....	22
4.6. Right to Easy Access to IIJ BCR-P.....	22
4.7. <i>Handling a Request from a Data Subject</i> .....	23
5. Complaint Handling Procedures .....	23
5.1. <i>Direct Complaints</i> .....	23
5.2. Indirect Complaints .....	23
6. Liability towards Third Party Beneficiaries.....	23
6.1. Third Party Beneficiary Rights.....	23
6.2. Liability of IIJ Lead Business Entity .....	24
6.3. <i>Liability and Enforceability in case of the IIJ Business Entity acting as a Data Controller</i> .....	25
6.4. Liability and Enforceability in case of the IIJ Business Entity acting as a Data Processor .....	25
6.5. Burden of Proof.....	25
7. Liability of IIJ Business Entities acting as Data Processors vis à vis Data Controllers .....	27
8. Cooperation Mechanism .....	28
8.1. Cooperation with the Data Controller .....	28
8.2. Cooperation with DPAs.....	28
8.3. <i>Notifications at the Time of Personal Data Breach</i> .....	29
9. Tools of Accountability and Data Protection for Projects (Data Protection by Design) .....	30
9.1. <i>Data Protection Impact Assessment</i> .....	30
9.2. Data Protection by Design and by Default.....	30
9.3. Development of Products and Services.....	30
9.4. Development of New Business and Mergers & Acquisitions .....	30
10. <i>[This section is not public.]</i> .....	31
11. <i>[This section is not public.]</i> .....	31
12. <i>[This section is not public.]</i> .....	31
13. <i>[This section is not public.]</i> .....	31
14. <i>[This section is not public.]</i> .....	31
15. <i>[This section is not public.]</i> .....	31
16. <i>[This section is not public.]</i> .....	31
16.1. <i>[This section is not public.]</i> .....	31
16.2. Records of Processing Activities .....	31

<i>17. [This section is not public.]</i> .....	32
<i>18. [This section is not public.]</i> .....	32
<i>19. [This section is not public.]</i> .....	32
Supplementary Provisions .....	32

## **1. Introduction**

### **1.1. Purpose**

In order to comply with the Regulation (EU) 2016/679 (General Data Protection Regulation, “**GDPR**”) and any applicable local laws implementing it, as well as to guarantee the highest level of protection for the personal data IJJ Business Entities (a list of which is available at [Annex 1](#)) process, as a Data Processor, IJJ has adopted these Binding Corporate Rules (the “**IJJ BCR-P**”).

### **1.2. Scope**

#### **1.2.1. Geographic Scope**

The IJJ BCR-P apply to the processing of Personal Data that are transferred directly or indirectly from within the EEA to an IJJ Business Entity outside the EEA, regardless of the nature of the Personal Data being processed. Specifically, the IJJ BCR-P applies to the Personal Data provided to the IJJ Business Entities by:

- (i) Data Controllers in the EEA which shall process personal data in accordance with the GDPR; or
- (ii) Data Controllers outside the EEA which shall process personal data in accordance with the GDPR due to the extraterritorial application of the GDPR or any other reasons, including the conclusion of the Standard Contractual Clauses.

The geographic scope of the IJJ BCR-P is comprised of all European Economic Area (“**EEA**”) member states as well as any other non-EEA countries in which IJJ Business Entities are present.

Where an IJJ Business Entity acts as a Data Processor, it shall be the sole responsibility of the Data Controller to determine whether to apply the BCR to (i) all personal data processed for processor activities that are subject to EEA law (e.g., data transferred from the EEA), or (ii) all personal data for processor activities, regardless of the origin of the data. Where an IJJ Business Entity acts as a Data Processor on behalf of another IJJ Business Entity acting as a Data Controller, the BCR shall apply to all personal data processed for processor activities, regardless of the origin of the data.

#### **1.2.2. Standing vis-à-vis IJJ Business Entities**

The IJJ BCR-P are a group policy legally binding vis-à-vis all IJJ Business Entities, by means of an Intra-Group agreement to which the IJJ Business Entities are parties. Each

IIJ Business Entity have a duty to respect the IIJ BCR-P. The IIJ Business Entities including their employees 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 BCR-P are a group policy which Executives and Others are bound to respect, as provided for in their employment contract. In order for Executives and Others to understand the details of the IIJ BCR-P and comply with them, 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 BCR-P are 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 BCR-P also comprise the Annexes listed in Section 19 which describe the procedures that guarantee the effective implementation of the IIJ BCR-P.

### **1.5. Keywords**

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

Term	Definition
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.
Data Exporter	IIJ Business Entity that acts as Data Controller and transfers Personal Data to a Data Importer located in a Third Country.
Data Importer	IIJ Business Entity that is located in a Third Country and that obtains Personal Data from the Data Exporter.

Term	Definition
Data Processor	Natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.
Data Protection Authorities (DPAs)	Any independent public authority based in the EEA which is authorized to handle data protection issues.
Data Subject	Identified or identifiable natural person whose Personal Data is processed.
EEA	The European Economic Area which consists of the EU member states and Iceland, Liechtenstein and Norway.
IIJ Lead Business Entity	IIJ Deutschland GmbH established and operating in Germany
Lead Data Protection Authority (Lead DPA)	North Rhine-Westphalia Commissioners for Data Protection and Freedom of Information (LDI NRW) in Germany
DPO	Data Protection Officer which has a responsibility to monitor compliance with the IIJ BCR-P and data protection law at a global level. If any events relevant to the IIJ BCR-P occur, the DPO shall report the 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 employees; part-time employees, etc.), officers (Directors, Auditors, etc.); and seconded employees of IIJ Business Entities.
IIJ	Internet Initiative Japan Inc.
IIJ Internal Audit Office	Internal audit department that is set up at IIJ.
IIJ BCR-P	Collective term referring to this document and to the Annexes that are stipulated in Section 19, 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 processor in one or more third countries within the IIJ Group.
IIJ Business Entities	Companies to which the IIJ BCR-P apply and which have



Term	Definition
or IIJ Business Entity	signed the Intragroup Agreement referred to in Section 1.2.3, a list of which is available in <u>Annex 1</u> .
IIJ Business Entity's Compliance Department	Departments in charge of general legal affairs and compliance that are set up at IIJ Business Entities, which may assist the IIJ Business Entity's Chief Privacy Office or IIJ Business Entity's CPO with the application of and compliance with local laws.
IIJ Business Entity's CPO	IIJ Business Entity's CPO is appointed by the IIJ Business Entity's President, and is responsible for the implementation of and operation of the IIJ BCR-P in the IIJ Business Entity. The IIJ Business Entity's CPO is assisted by the IIJ Business Entity's Chief Privacy Office.
IIJ Business Entity's Chief Privacy Office	Security control departments that are set up in 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 CPO, and IIJ CPO, in giving instructions to the IIJ Business Entity's departments that process Personal Data, including guidance, implementation of risk assessment and internal audits. It 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. The IIJ Business Entity's Chief Privacy Office can seek for advice from IIJ CPO, if necessary.
IIJ CPO	Chief Privacy Officer in IIJ who has the responsibility and authority for providing advice and assistance on the overall implementation and operation of the IIJ BCR-P for IIJ Business Entities, supervising the implementation of the IIJ BCR-P by IIJ Business Entities and reporting the circumstances of the implementation to the DPO, and ensuring that IIJ Business Entities are informed of instructions and advice from the DPO, assessing a data processing activity reported for approval and conducting a DPIA for a data processing activity, as appropriate, assessing a transfer of personal data reported for approval and preparing the requisite documentation, preparing

Term	Definition
	a response to an exercise of rights by a Data Subject, assessing a security incident or a personal data breach and possible related regulatory obligations, dealing with the data protection authorities' investigations.
IIJ Compliance Department	Department in charge of general legal affairs and compliance that is set up at IIJ.
IIJ Chief Privacy Office	Security control department that is set up at IIJ. It has the role of ensuring data protection as well as supervising the security control of IIJ Business Entities.
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 these IIJ BCR-P.
Personal Data Processing	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.
Personal Data Transfer	The disclosure of, the transmission to, or the making available to an IIJ Business Entity (as listed in <u>Annex 1</u> ) in a Third Country of Personal Data collected in the EEA.
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	All non-EEA countries.

Term	Definition
Third Countries	
Third Party	Natural or legal person, public authority, agency or body other than the Data Subject, the Data Controller, the Data Processor, an IIJ Business Entity, and persons who, under the direct authority of the Data Controller or the Data Processor, are authorised to process Personal Data
Third Party Beneficiaries	Data Subjects and persons who may exercise their rights under the IIJ BCR-P, excluding the person who is defined as Third Party.

## 2. General Principles of Personal Data Processing

**General principle.** The principles set out in the IJJ BCR-P shall be respected by IJJ Business Entities irrespective of local laws, except where local laws include more stringent requirements than those set up in the IJJ BCR-P. Where there are aspects of the IJJ BCR-P that are subject to more stringent local laws, the more stringent laws will apply to these aspects.

**Data Processors.** If an IJJ Business Entity acts as a Data Processor, in addition to the IJJ BCR-P, it shall comply with the data processing procedures and security measures agreed to with the Data Controller. The IJJ Business Entity acting as a Data Processor (including any Executives and Others of the IJJ Business Entity) has a duty to respect the instructions of the Data Controller for processing, security and confidentiality, as well as for transfers of Personal Data to third countries. If, for any reason, the IJJ Business Entity (or any Executives and Others of the IJJ 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 IJJ BCR-P.** If an IJJ Business Entity as a Data Processor, has reasons to believe that applicable legislation prevents it from fulfilling its obligations under the IJJ BCR-P and/or the instructions from the Data Controller, or would have a substantial effect on the guarantees provided by the IJJ BCR-P, the person in charge of each IJJ Business Entity shall promptly inform the Data Controller and the IJJ Lead Business Entity, and seek support at that IJJ Business Entity's Chief Privacy Office by electronic mail or in writing. In case of doubt as to the application of the IJJ BCR-P and local laws, and where these conflicts cannot be quickly resolved, the IJJ Business Entity's Chief Privacy Office will correspond with the competent Data Protection Authority.

Further, if the IJJ Business Entity has reason to believe that legal requirements it may be subject to in non-EEA countries are likely to have a substantial adverse effect on the guarantees provided by the IJJ BCR-P (including legally binding requests for disclosure of Personal Data by a law enforcement authority or state security body), the IJJ Business Entity will promptly inform the relevant data protection authorities for the Controller and the Processors about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure of personal data by a 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 relevant Data Protection Authority and, where required, the Data Controller. In such cases, the IIJ Business Entity will use its best efforts to obtain the right to waive such obligation and communicate as much information to the competent Data Protection Authority as soon as possible, and demonstrate its efforts thereto. If, despite IIJ's best efforts, it is not in a position to notify the competent Data Protection Authority, it will provide general information on the requests it receives at least once a year, in accordance with the procedure set out in Section 16. In any event, where IIJ is obliged to provide Personal Data to a public authority, this 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 competent Data Protection Authority 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.

If the IIJ Business Entity acts as a Data Processor, it will notify the Data Controller, unless the relevant law prohibits the IIJ Business Entity from doing so on important grounds of public interest. If necessary, while cooperating with the Data Controller, it will also notify the local DPA.

**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 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. IIJ Chief Privacy Office shall, in cooperation with the DPO, take action to resolve that issue within two months of having received such escalation.

#### *2.1. Legal Basis for Personal Data Processing*

*[Section intentionally blank in IIJ BCR-P]*

## **2.2. General Principles relating to processing of Personal Data**

The IIJ Business Entity as a Data Processor will comply with the general principles above 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:

- i. have a general duty to help and assist the Data Controller to comply with the law, including assistance to be transparent about sub-processor activities in order to allow the Data Controller to correctly inform the Data Subjects.
- ii. only process Personal Data in accordance with the documented instructions of the Data Controller, including as regards transfers of Personal Data to a third country, unless it is required to process Personal Data under the EU or EEA member state laws to which it is subject. In such case, IIJ shall inform the Data Controller of that legal requirement before processing takes place unless the EU or EEA member state laws prohibit such disclosure on important grounds of public interest. Each IIJ Business Entity listed in Annex 1 acting as Data Processor, and their employees, shall respect the instructions from the Data Controller regarding the data processing and the security and confidentiality measures;
- iii. erase, anonymise, update or rectify Personal Data, when required to do so on instruction from the Data Controller, as required under the terms of its contract with that Data Controller;
- iv. notify accordingly other IIJ Business Entities or any external sub-processor to whom the Personal Data has been disclosed, so that they can also update their records;
- v. comply with the security and organizational measures to ensure a level of security appropriate to the risks presented by processing, which at least meet the requirements of the EU or EEA member state laws and any existing particular measures specified in the contract;
- vi. assist the controller in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with

- the requirements set up by the IJJ BCR-P in practice such as data protection by design and by default
- vii. inform the Data Controller of any security breach without undue delay;
  - viii. 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 obligation to respond to requests for exercising the Data Subjects rights in the compliance with its duty to inform Data Subjects and respect Data Subjects' rights; and 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;
  - ix. arrange the sub-processing of Personal Data by other IJJ Business Entities or by Third Parties only with the prior information of the Data Controller and its prior written general or specific consent;
  - x. in the case of transfers or Data Processor relationships with Third Parties acting as sub-processors or with an IJJ Business Entity, acting as sub-processor (which IJJ Business Entity is not party to the Service Agreement), the sub-processing may be permissible only with the prior informed specific or general written authorization of the Data Controller. 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 this case, the IJJ Business Entities shall enter into written agreements, which provides that adequate protection is provided as set out in Article 28, 29, 32, 45, 46, 47 of the GDPR and ensures that the same data protection obligations as set out in the Service Agreement between the Data Controller and the IJJ Business Entity and also in the IJJ BCR-P are imposed on the Third Party or the IJJ Business Entity acting as sub-processor, whereby:
    - The Third Party must not process the Personal Data except on instructions from the IJJ Business Entity, unless he is required to do so by law.
    - The Third Party 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 shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
  - The Third Party must comply with Section 3.5 prior to effecting any transfer of Personal Data outside the EEA;
  - The Third Party must accept that its facilities may be audited by the Data Controller, 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.
- xi. inform promptly the Data Controller of its inability to process Personal Data on its behalf and to comply with its instructions, including where IJJ has reason to believe that existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Data Controller or other obligations under the BCR, in which case the Data Controller will be entitled to suspend the transfer of Personal Data and/or terminate the contract.

Further, if the contract of the Data Processor is cancelled or otherwise terminated, the IJJ Business Entity will, in accordance with the instructions of the Data Controller, certify to the Data Controller that it has returned or destroyed all of the Personal Data that had been transferred as well as all copies, unless applicable EU or EEA member state law prevents returning or destroying all or part of the Personal Data transferred, in which case it 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 IJJ BCR-P]*

### *2.4. Processing the Personal Data of Children*

*[Section intentionally blank in IJJ BCR-P]*

### *2.5. Processing Sensitive Data*

*[Section intentionally blank in IJJ BCR-P]*

## **2.6. Security**

### **2.6.1 General Security Policies**

The IJJ 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, the IJJ Business Entity shall comply with the requirements in the IJJ Group Security Policy, as revised and updated from time to time, together with any other security procedures relevant to a business area or function. The IJJ Business Entity will implement and comply with breach notification policies as required by the applicable data protection law in the EEA. Furthermore, the IJJ Business Entity will ensure that providers of services to that Entity also adopt appropriate and equivalent security measures.

### **2.6.2 Personal Data Breach**

Where there is a breach of security or confidentiality that affects the Personal Data of individuals, the IJJ 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 IJJ CPO, and ultimately the DPO. IJJ shall make the materials available to the competent Data Protection Authority upon request.

IJJ Business Entity as a Data Processor shall inform the Data Controller without undue delay after becoming aware of any personal data breach. In addition, the IJJ Business Entity as a sub-processor shall have the duty to inform the Data Processor and the Data Controller without undue delay after becoming aware of any personal data breach.

If the IJJ Business Entity is the Data Processor, it shall:

- cooperate with the Data Controller, and make sure that it complies with the security requirements prescribed by the Data Controller;
- assist the Data Controller in complying with its obligations under applicable EU or EEA member state laws without undue delay and to the extent reasonably possible;
- comply with the requirements of the Data Controller regarding the appointment of any sub-processor. The IJJ Business Entity will also ensure that sub-processors undertake to comply with provisions which are consistent with (i) the terms in its contracts with the Data Controller and (ii) the IJJ BCR-P, 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; and
- notify the Data Controller of any security breach, in accordance with the terms of the

contract with that Data Controller.

*2.7. Automated Individual Decisions*

*[Section intentionally blank in IJ BCR-P]*

**2.8. 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 the BCR.

### 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, the IIJ BCR-P applies to transfer of Personal Data of customers (and their customers), suppliers and service providers, and of Executives and Others, and employees, to and between the IIJ Business Entities, and to third party processors appointed by IIJ Business Entities.

The types of entities and the categories of data covered by these BCR include the following:

- **Customers 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 customer, (2) Case manager of IIJ Business Entity browses customer data and processes the 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.

- **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 IJJ Business Entity receives customer data from customer by means specified by customer, (2) Case manager of IJJ Business Entity browses customer data and processes the personal data, according to the procedure specified by customer.  
Case 2: (1) Client sends customer data on cloud service (SaaS) provided by IJJ Business Entity and processing of data sent on service is performed (2) The case manager of IJJ Business Entity does not have access to the data stored by the customer normally, but access may be granted to the 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 IJJ Business Entity, and customer stores customer data on the environment, (2) The case manager of IJJ 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.
- **Personal data of IJJ's suppliers and service providers** (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 IJJ Business Entities
- Types of processing: (1) Case manager of IJJ 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 IJJ Business Entity digitalizes or stores such data in the area accessible only to the parties concerned. (3) The parties concerned in IJJ Business Entity may browse personal data of the suppliers' or service provider's personnel stored for supplier registration, purchase order process, purchase invoicing.

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

Personal data is transferred from the EEA to non-EEA territories within the scope of the IJJ Business Entity. For example, for customer services, to provide IaaS and email outsourcing services, to provide human resources management, or for announcements on

personnel changes and recruitment, where data transfer is necessary.

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 the transfer of Personal Data to and between the IIJ Business Entities and to a Third Party within or outside the EEA.

*3.1. Personal Data Transfer from an IIJ Business Entity acting as a Data Controller located within or outside the EEA to an IIJ Business Entity located within or outside the EEA*

*[Section intentionally blank in IIJ BCR-P]*

*3.2. Personal Data Transfer from an IIJ Business Entity acting as a Data Controller, located within or outside of EEA to a Third Party located within or outside of EEA*

*[Section intentionally blank in IIJ BCR-P]*

### **3.3. Personal Data Transfer from Data Controller within or outside the EEA to an IIJ Business Entity located within or outside the EEA**

The IIJ Business Entity as a Data Processor receives Personal Data from Data Controller within or outside the EEA. IIJ Business Entity as Data Processor should enter into a Service Agreement with the Data Controller, and the IIJ 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 EEA to an IIJ Business Entity located within or outside the EEA**

The IIJ Business Entity as a Data Processor transfers Personal Data to another IIJ Business Entity acting as sub-processor located outside the EEA, the transfer is covered by the IIJ BCR-P.

IIJ Business Entity as Data Processor should also enter into a written agreement, referred to in Section 2.2. of the BCR, with 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 EEA to a Third Party located within or outside the EEA**

The IIJ Business Entity as a Data Processor, transfers Personal Data to a Third Party, the IIJ Business Entity transferring the Personal Data shall ensure that the Third Party receiving the Personal Data commits in writing to providing sufficient guarantees in respect of the technical security, confidentiality and organisational measures governing the processing of the Personal Data (see Section 2.2).

Third Parties must also commit in writing not to transfer any Personal Data except if based on a framework compliant with the applicable data protection regulations in the EEA, in particular:

1. That the Third Party transfers the data to a country that has been considered by a Decision of the European Commission to confer an adequate level of protection to Personal Data, or
2. That the Third Party establishes a legally recognized framework to lawfully transfer the data outside the EEA, or
3. That any of the derogations foreseen by the GDPR applies.

#### **4. Rights of Data Subject**

##### *4.1. Right of access by the Data Subject*

*[Section intentionally blank in IIJ BCR-P]*

##### *4.2. Right to Rectification*

*[Section intentionally blank in IIJ BCR-P]*

##### *4.3. Right to Erasure (Right to be Forgotten)*

*[Section intentionally blank in IIJ BCR-P]*

##### *4.4. Right to Restriction of Processing*

*[Section intentionally blank in IIJ BCR-P]*

##### *4.5 Direct Marketing*

*[Section intentionally blank in IIJ BCR-P]*

#### **4.6. Right to Easy Access to IIJ BCR-P**

All Data Subjects have the right to have easy access to the IIJ BCR-P. For this reason, the parts of the IIJ BCR-P which are relevant for the Data Subjects will be published on the website of IIJ. For Executives and Others the IIJ BCR-P will also be made available on the intranet. The parts of the IIJ BCR-P to be published are as follows:

- Section 1, 2, 3, 4, 5, 6, 7, 8, 9 and 16.2;
- Annex 1, 4 and 5.

The information should be provided in full, summary is not sufficient.

#### *4.7. Handling a Request from a Data Subject*

*[Section intentionally blank in IJJ BCR-P]*

## **5. Complaint Handling Procedures**

### *5.1. Direct Complaints*

*[Section intentionally blank in IJJ BCR-P]*

### **5.2. Indirect Complaints**

If the Data Subject has filed a complaint against the processing of his/her Personal Data by an IJJ Business Entity acting as a Data Processor that IJJ Business Entity will actively support the complaint processing response that the Data Controller carries out.

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

Where an IJJ 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 IJJ Business Entity will undertake to handle the complaint in accordance with the procedures stipulated in Annex 5.

In such event, where the IJJ Business Entity as a Data Processor handles complaints, these shall be dealt without undue delay and in any event within one month by the IJJ Business Entity's CPO. Taking into account the complexity and number of the requests, the time frame for response can be extended by two further months at the utmost. In such case, the data subject should be informed accordingly.

## **6. Liability towards Third Party Beneficiaries**

### **6.1. Third Party Beneficiary Rights**

It is acknowledged the right of Data Subjects whose personal data is processed by an IJJ Business Entity, and the right of Data Controllers for which an IJJ Business Entity acts as a Data Processor are enforceable under the IJJ BCR-P as Third Party Beneficiaries in the event of a breach by IJJ Business Entities of *any* of its commitments therein, including:

- Purpose limitation (Section 2.2 of the IJJ BCR-P),
- Data quality and proportionality (Section 2.2 of the IJJ BCR-P),
- Criteria for making the processing legitimate (Section 2.1 of the IJJ BCR-P),
- Transparency and easy access to BCR (Section 2.3 of the IJJ BCR-P),

- Processing of Sensitive Data (Sections 2.4 and 2.5 of the IJJ BCR-P),
- Rights of access, rectification, erasure, restriction and objection to the processing (Section 4 of the IJJ BCR-P),
- Rights in case automated individual decisions are taken (Section 2.7 of the IJJ BCR-P),
- Security and confidentiality (Section 2.6 of the IJJ BCR-P),
- Restrictions on onward transfers outside of the group of companies (Section 3 of the IJJ BCR-P),
- National legislation preventing respect of BCR (Section 2 of the IJJ BCR-P),
- Right to complain through the internal complaint mechanism of the companies (Section 5 of the IJJ BCR-P),
- Cooperation with the Data Controller (Section 8.1 of the IJJ BCR-P),
- Cooperation duties with Data Protection Authority (Section 8.2 of the IJJ BCR-P),
- Liability and jurisdiction provisions (Section 6 of the IJJ BCR-P),
- Data protection by design and by default (Section 9.2 of the IJJ BCR-P).

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 for judicial remedy to the competent courts of the jurisdiction. Where an IJJ 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, unless the legal obligations of the Data Controller and the Data Subject are assumed by another entity, the Data Subject will be entitled to enforce the IJJ BCR-P against the IJJ 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 IJJ Lead Business Entity**

The IJJ Lead Business Entity shall in particular be responsible for and agree to take the necessary action to remedy the acts of other non-EEA IJJ Business Entities or the breaches caused by external sub-processor established outside of the EEA and to pay compensation for any damages resulting from the violation of the BCR-P by non-EEA IJJ Business



Entities or external sub-processors established outside the EEA. In this regard, the IJJ Lead Business Entity shall accept liability as if the violation had taken place by itself in the EEA Member State in which it is based instead of the IJJ Business Entity outside the EEA or the external sub-processor established outside the EEA. Further, the IJJ Lead Business Entity shall not be entitled to rely on a breach by an IJJ Business Entity established outside the EEA or external sub-processor established outside the EEA of its obligations in order to avoid its own liabilities. However, if the IJJ Lead Business Entity can prove that the IJJ Business Entity outside the EEA or the external sub-processor established outside the EEA is not liable for the violation, it may discharge itself from any responsibility.

*6.3. Liability and Enforceability in case of the IJJ Business Entity acting as a Data Controller*

*[Section intentionally blank in IJJ BCR-P]*

**6.4. Liability and Enforceability in case of the IJJ Business Entity acting as a Data Processor**

Where an IJJ Business Entity is acting as a Data Processor, IJJ Lead Business Entity bears liability for the damage that has occurred only if it has not followed the instructions of the Data Controller, or if it has breached the IJJ BCR-P. The Data Subjects may exercise their right to enforce the IJJ BCR-P and the instructions of the Data Controller, to obtain redress and to receive compensation before the courts of the EEA Member State (i) where the IJJ Lead Business Entity is established, or (ii) where the Data Subject has his/her habitual residence. In addition, Data Subjects have the right to lodge a complaint before a competent DPA in particular in the EEA Member State (i) of their habitual residence, (ii) place of work or (iii) place of the alleged infringement. In particular, the Data Subject may directly enforce the BCR against the IJJ Business Entity acting as the Data Processor, or IJJ Lead Business Entity where the IJJ BCR-P impose obligations on Data Processors, particularly Sections 2, 4-7 and 8.2, as well as Annex 5.

**6.5. Burden of Proof**

The IJJ Lead Business Entity will have the burden of proof to demonstrate that IJJ Business Entity outside the EEA or the external sub-processor outside the EEA is not liable for any violation of the BCR-P which has resulted in the Data Subject claiming damages. Further, where the Data Subjects have claimed that they have suffered damage as a likely result of a breach of the IJJ BCR-P, IJJ Lead Business Entity accepts to bear the burden of proof for demonstrating that the IJJ Business Entity outside the EEA or the external sub-processor outside the EEA is not responsible for the breach of the BCR

giving rise to those damages or that no such breach took place.

## **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 contract between both entities.

Where the IIJ Business Entity, acting as a Data Processor, has failed to comply with the IIJ BCR-P or with the Data Controller's instructions, or with the Service Agreement, the Data Controller has the right to enforce the IIJ BCR-P against IIJ Lead Business Entity, as provided for in Section 6 of the IIJ BCR-P and in the contract that the Data Controller has concluded with the IIJ Business Entity. The Data Controller has the right to enforce the IIJ BCR-P against IIJ Lead Business Entity in case any Third Party acting as sub-processor, established outside of the EEA breaches the written agreement referred to in Section 2.2. of the IIJ BCR-P.

The Data Controller shall have rights to have judicial remedies to obtain redress and compensation, as described in Section 6.1, 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, to a reasonable extent and within a reasonable time in any case, without undue delay, provide the Data Controller with information regarding the Personal Data Processing, in order to enable the Data Controller to comply with the applicable data protection law in the EEA.

Where an IIJ Business Entity acts as a Data Processor or a sub-processor, the IIJ Business Entity shall cooperate with and assist the Data Controller in complying and demonstrating compliance with the law (such as its duty to respect the Data Subjects or to handle their complaints, or to be in a position to reply to investigation or inquiry from the DPA ). This shall be done in a reasonable time and to the extent reasonably possible.

Furthermore, where an IIJ Business Entity acts as a Data Processor or a sub-processor, it shall cooperate with the Data Controller when the Data Controller instructs that, for the disposal, deletion or return of Personal Data to the Data Controller, as well as the IIJ Business Entity shall assist the Data Controller in ensuring compliance with the obligations concerning the security of processing, personal data breach, data protection impact assessment and prior consultation (Article 32-36 GDPR).

### **8.2. Cooperation with DPAs**

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 competent DPAs in the context of investigations or inquiries.

IIJ Business Entities shall actively cooperate with the competent DPAs in the performance of their tasks and particularly in order to ensure adequate and timely replies to requests received from the competent DPAs. IIJ Business Entities also accept to be audited by the competent DPAs to verify compliance with the applicable data protection law in the EEA and with these BCR.

IIJ Business Entities shall make available to the competent DPAs 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 competent DPAs on any issues

regarding data protection.

*8.3. Notifications at the Time of Personal Data Breach*

*[Section intentionally blank in IJ 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 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 IIJ 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. [This section is not public.]*

*11. [This section is not public.]*

*12. [This section is not public.]*

*13. [This section is not public.]*

*14. [This section is not public.]*

*15. [This section is not public.]*

*16. [This section is not public.]*

*16.1. [This section is not public.]*

## **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 as Data Processor. That record shall contain all of the following information:

- the name and contact details of the Processors and the Sub-Processors and of the Data Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the DPO;
- the categories of processing carried out on behalf of the Data Controller;
- where applicable, transfers of personal data 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 GDPR, the documentation of suitable safeguards;
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

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

*17. [This section is not public.]*

*18. [This section is not public.]*

*19. [This section is not public.]*

END

### **Supplementary Provisions**

The IIJ BCR-P are enacted from (Date).