IIJ BCR-C

（Controller Policy）

Version 1.0

28th July 2021

Internet Initiative Japan Inc.

Version No.	Revision Date	Revision Reason & Details	Approval	Creation/Revision
Ver. 1.0	28th July 2021	Initial Version	Miyoshi	IIJ Chief Privacy Office

Table of Contents

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 IIJ Business Entities (a list of which is available at Annex 1) process, as a Data Controller, IIJ has adopted these Binding Corporate Rules (the "**IIJ BCR-C**").

1.2. Scope

1.2.1. Geographic Scope

The IIJ BCR-C apply to the processing of Personal Data that are transferred directly or indirectly from within the EEA to an IIJ Business Entity as a Data Controller or Data Processor outside the EEA, regardless of the nature of the Personal Data being processed. The geographic scope of the IIJ BCR-C is comprised of all European Economic Area ("**EEA**") member states as well as any other non-EEA countries in which IIJ Business Entities are present.

1.2.2. Standing vis-à-vis IIJ Business Entities

The IIJ BCR-C are 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 have a duty to respect the IIJ BCR-C

1.2.3. Standing vis-à-vis Employees

The IIJ BCR-C 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-C 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.

1.2.4. Standing vis-à-vis Customers

[Section intentionally blank in IIJ BCR-C]

1.3. Document Retention and Distribution

The IIJ BCR-C are made available to Executives and Others and will be communicated

to customers and the Data Subjects upon request as specified in Section 4.

1.4. Related Documents

The IIJ BCR-C also comprise the Annexes listed in Section 19 which describe the procedures that guarantee the effective implementation of the IIJ BCR-C.

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.
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-C and data protection law at a global level. If any events relevant to the IIJ BCR-C occur,

Term	Definition
	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-C	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 Controller for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within the IIJ Group.
IIJ Business Entities or IIJ Business Entity	Companies to which the IIJ BCR-C apply and which have signed the Intragroup Agreement referred to in Section 1.2.3, a list of which 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 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-C 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

Term	Definition
	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-C for IIJ Business Entities, supervising the implementation of the IIJ BCR-C 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 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

Term	Definition
	have the same meaning as the term "Personal Data" in the context of the issues regulated in these IIJ BCR-C.
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 Annex 1)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 Third Countries	All non-EEA 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-C, excluding the person who is defined as Third Party.

2. General Principles of Personal Data Processing

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

Relationship between National Law and the IIJ BCR-C. If an IIJ Business Entity has reasons to believe that applicable legislation prevents it from fulfilling its obligations under the IIJ BCR-C, or would have a substantial effect on the guarantees provided by the IIJ BCR-C, the person in charge of each IIJ Business Entity shall promptly inform the IIJ Lead Business Entity of the issue and seek support at that IIJ Business Entity's Chief Privacy Office by electronic mail or in writing. In case of doubt as to the application of the IIJ BCR-C and local laws, and where these conflicts cannot be quickly resolved, the IIJ Business Entity's Chief Privacy Office will correspond with the competent Data Protection Authority.

Further, if the IIJ 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 IIJ BCR-C (including legally binding requests for disclosure of Personal Data by a law enforcement authority or state security body), the IIJ Business Entity will promptly inform the relevant data protection authority 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. 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 the IIJ Business Entity'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 the IIJ Business Entity 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.

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

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

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

Subject which require protection of Personal Data, in particular where the Data Subject is a child.

2.2. General Principles relating to processing of Personal Data

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

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

2.3. Collection of Personal Data

Where an IIJ Business Entity collects Personal Data relating to a Data Subject from the Data Subject, the IIJ Business Entity shall, at the time when Personal Data are obtained, provide the Data Subject with all of the following information:

- the identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative and DPO;
- the purposes of the processing for which the Personal Data are intended, as well as the legal basis for the processing;

- if processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party, the legitimate interests pursued by the Data Controller or a Third Party;
- the recipients or categories of recipients of the Personal Data, if any;
- where applicable, the fact that the Data Controller intends to transfer Personal Data to a Third Country or international organisation and the existence or absence of an adequacy decision by the European Commission. In the latter case, the IIJ Business Entity shall also refer, when required to do so by the applicable data protection law in the EEA, to the appropriate or suitable safeguards and the means to obtain a copy thereof or where they have been made available.

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

- the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the Data Controller access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
- where the processing is based on the Consent of the Data Subject, as provided for in the applicable data protection law in the EEA, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of processing based on Consent before its withdrawal;
- the right to lodge a complaint in accordance with the procedure set out in Section 5 and Annex 5, and/or with a DPA;
- whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, referred to in the applicable data protection law in the EEA and, at least in those cases,

meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

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

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

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

The IIJ Business Entity should provide this information:

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

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

The IIJ Business Entity will follow this Section 2.3, unless there is a legal basis under the EU or EEA member state laws for not doing so (for example, where it is necessary to safeguard national security or defence, for the prevention or detection of crime, taxation purposes, judicial proceedings).

2.4. Processing the Personal Data of Children

Where processing is based on Consent, in relation to the offer of information society services directly to a child below the age of sixteen years (or a lower age, as set by the

laws of the EEA Member State applicable to the processing in question), processing of Personal Data shall be possible only if and to the extent that Consent is given or authorised by the holder of parental responsibility over the child. The IIJ Business Entity shall make reasonable efforts to verify in such cases that Consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

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

2.5. Processing Sensitive Data

IIJ Business Entity can process Sensitive Data only where:

- the Data Subject has given explicit Consent to the processing of this Personal Data for one or more specified purposes, except where the applicable EU or EEA member state laws provide that the processing of such data is prohibited and that the prohibition may not be lifted by the Data Subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by EU or EEA member state law or a collective agreement pursuant to EEA member state law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
- processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the Consent of the Data Subjects;

- processing relates to Personal Data which is manifestly made public by the Data Subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of EU or EEA member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or EEA member state law or pursuant to contract with a health professional and subject to the conditions and safeguards provided by the applicable data protection law in the EEA ;
- processing is necessary for reasons of public interests in the area of public health, on the basis of EU or EEA member state law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy; or
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the applicable EU or EEA member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

2.6. Security

2.6.1 General Security Policies

The 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, the 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. The IIJ Business Entity will implement and comply with breach notification policies as required by the applicable data protection law in the EEA. Furthermore, the IIJ Business Entity will ensure that providers of services to that Entity also adopt appropriate and equivalent security measures by concluding contracts which obliges the providers to adopt such measures and any other means.

2.6.2 Personal Data Breach

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

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

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

2.7. Procedures ensuring compliance with the Principles of Section 2

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

3. Transfer of Personal Data

IIJ Business Entities, 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, will transfer Personal Data of customers (and their customers), suppliers and service providers, and of Executives and Others, and employees, to other IIJ Business Entities or third party processors appointed by IIJ Business Entities.

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

- **Employee data** (name, gender, address, phone number, email address, data of birth, work experience, salary)
- Purpose of processing: To conduct personnel management of employees of IIJ Business Entity.
- Data subjects: employees of IIJ Business Entities
- Types of processing: (1) The employee who works at the site in the EEA or the personnel manager at the site in the EEA sends by emails personal data of the employee working at the entities in the EEA to the personnel manager at the IIJ Business Entity outside the EEA, (2) HR manager of IIJ Business Entity outside the EEA stores the received employee data in an area accessible only to the concerned parties, (3) the personnel manager in charge of the IIJ Business Entities outside the EEA reviews and processes employee data for personnel management (training, personnel evaluation, transfer and promotion, placement management, etc.).

- **Personal data of IIJ'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 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.

- **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:
- (1) Case personnel in charge of IIJ Business Entity receive customer data from customers by business card or email;
  (2) Case manager of IIJ Business Entity digitalizes or stores such data in the area accessible only to the parties concerned. (3) The parties concerned of the IIJ Business Entity store the data and browse and process the stored customer data for quotation, order receipt, purchase, billing and marketing.

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 IIJ 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 from the EEA to 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

Where an IIJ Business Entity, acting as a Data Controller, transfers Personal Data to another IIJ Business Entity located outside the EEA, the transfer is covered by the IIJ BCR-C.

Where the IIJ Business Entity, acting as Data Controller shares Personal Data with IIJ Business Entity as a Data Processor, the IIJ Business Entity acting as Data Controller shall put in place an agreement with the IIJ Business Entity as a Data Processor that at

minimum meets the requirements of Article 28 of the GDPR.

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

Any time an IIJ Business Entity, acting as a Data Controller, permits a Third Party to process Personal Data from the EEA, it shall (i) ensure that the Third Party is bound by law to appropriate duties of confidentiality and data security at least equal to those required by the GDPR, and/or (ii) impose such obligations by way of contract with the Third Party. The Third Party must commit to only transfer Personal Data to other Third Parties outside the EEA in compliance with the GDPR (unless it is already subject to a legal obligation to do so). Where the Third Party is a Data Processor, the IIJ Business Entity shall put in place an agreement with the Third Party that at minimum meets the requirements of Article 28 of the GDPR.

If an IIJ Business Entity, acting as a Data Controller, transfers Personal Data to a Third Party located outside the EEA, the IIJ Business Entity transferring the Personal Data shall ensure compliance with Section 3 of this BCR and either (i) shall rely on an adequacy decision decided by the European Commission according to Articles 45 of the GDPR, (ii) shall also ensure that it signs the appropriate Standard Contractual Clauses adopted by the European Commission (provided for in Commission Decision dated 15 June 2001 (2001/497/EC) (including the amendment subject to the Commission Implementing Decision (EU) 2016/2297 dated 16 December 2016) and dated 24 December 2004 (2004/915/EC)), where another Data Controller receives that Personal Data, or it signs the appropriate Standard Contractual Clauses adopted by the European Commission (provided for in Commission Decision dated 5 February 2010 (2010/87/EU)) (including the amendment subject to the Commission Implementing Decision (EU) 2016/2297 dated 16 December 2016), where a Data Processor receives that Personal Data, (iii) shall put in place another appropriate safeguard Article 46, 47, or 48 of the GDPR, or (iv) shall ensure that a derogation according to Article 49 of the GDPR applies.

3.3. 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

[Section intentionally blank in IIJ BCR-C]

3.4. 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

[Section intentionally blank in IIJ BCR-C]

4. Rights of Data Subject

4.1. Right of access by the Data Subject

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

4.2. Right to Rectification

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

4.3. Right to Erasure (Right to be Forgotten)

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

- the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; However, it does not apply where the IIJ Business Entity acting as a Data Controller is not required, by the applicable

data protection law in the EEA, to erase the Personal Data (e.g. when that processing is necessary for reasons of public interest in the area of public health or for the establishment, exercise or defense of legal claims).

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

4.4. Right to Restriction of Processing

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

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

4.5 Right to data portability

The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the IIJ Business Entities, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Data Controller without hindrance from the IIJ Business Entities to which the personal data have been provided, where:

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

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

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

4.6 Right to Object

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

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

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

4.7 Automated Individual Decisions

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

1. Where this is necessary for entering into, or performing, a contract between the IIJ Business Entity and the Data Subject;

2. Where this is authorized by EU or EEA member state law to which the IIJ Business Entity is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests.
3. This is based on the Data Subject's explicit consent.

The Data Controller shall implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Data Controller, to express his or her point of view and to contest the decision in the cases referred to in points 1 and 2 above.
The automated decisions shall not be based on Sensitive Data, unless Article 9(2)(a) or (g) of the GDPR applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

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

4.8. Right to Easy Access to IIJ BCR-C

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

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

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

4.9. Handling a Request from a Data Subject

If a request stipulated in this Section has been made, the IIJ Business Entity that is acting as a Data Controller shall acknowledge receipt promptly, and provide a substantive response, without undue delay and at the latest within one month, with the reasons for not taking action (where applicable), the possibility of lodging a complaint with a DPA, and seeking a judicial remedy, in accordance with the procedures stipulated in Annex 4 "Rules Regarding the Data Subject's Personal Data Rights."

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

5. Complaint Handling Procedures

5.1. Direct Complaints

If a complaint has been filed by a Data Subject, alleging that their Personal Data has not been processed in accordance with the IIJ BCR-C or the applicable data protection law in the EEA, the IIJ Business Entity will handle that complaint in accordance with the procedures stipulated in Annex 5 “Procedures Regarding Complaints and Consultations Regarding Personal Data.”

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

5.2. Indirect Complaints

No description as a Data Controller

6. Liability towards Third Party Beneficiaries

6.1. Third Party Beneficiary Rights

It is acknowledged the right of Data Subjects whose personal data is processed by an IIJ Business Entity are enforceable under the IIJ BCR-C as Third Party Beneficiaries in the event of a breach by IIJ Business Entities of *any* of its commitments therein, including:

- Purpose limitation (Section 2.2 of the IIJ BCR-C),
- Data quality and proportionality (Section 2.2 of the IIJ BCR-C),
- Criteria for making the processing legitimate (Section 2.1 of the IIJ BCR-C),
- Transparency and easy access to BCR (Section 2.3 of the IIJ BCR-C),
- Processing of Sensitive Data (Sections 2.4 and 2.5 of the IIJ BCR-C),
- Rights of access, rectification, erasure, restriction and objection to the processing (Section 4 of the IIJ BCR-C),
- Rights in case automated individual decisions are taken (Section 2.7 of the IIJ BCR-C),
- Security and confidentiality (Section 2.6 of the IIJ BCR-C),
- Restrictions on onward transfers outside of the group of companies (Section 3 of the IIJ BCR-C),
- National legislation preventing respect of BCR (Section 2 of the IIJ BCR-C),
- Right to complain through the internal complaint mechanism of the companies (Section 5 of the IIJ BCR-C),
- Cooperation duties with Data Protection Authority (Section 8.2 of the IIJ BCR-C),
- Liability and jurisdiction provisions (Section 6 of the IIJ BCR-C),
- Data protection by design and by default (Section 9.2 of the IIJ BCR-C).

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 before courts or the competent DPA as set out in Section 6.3.

6.2. Liability of IIJ Lead Business Entity

The IIJ Lead Business Entity shall in particular be responsible for and agree to take the necessary action to remedy the acts of other non-EEA IIJ Business Entities to pay compensation for any damages resulting from the violation of the BCR-C by non-EEA IIJ Business Entities. In this regard, the IIJ 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 IIJ Business Entity outside the EEA.

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

6.3. Liability and Enforceability in case of the IIJ Business Entity

The Data Subject may exercise their right to enforce the IIJ BCR-C, to obtain redress and to receive compensation before the courts of the EEA Member State (i) where IIJ Lead Business Entity is established, or (ii) where the Data Subject has his/her habitual residence. In addition, the Data Subjects have the right to lodge a complaint before a competent DPA in particular in the EEA Member State of (i) their habitual residence, (ii) place of work, or (iii) place of the alleged infringement.

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

[Section intentionally blank in IIJ BCR-C]

6.5. Burden of Proof

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

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

[Section intentionally blank in IIJ BCR-C]

8. Cooperation Mechanism

8.1. Cooperation with the Data Controller

[Section intentionally blank in IIJ BCR-C]

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 DPAs in the context of investigations or inquiries.

IIJ Business Entities shall actively cooperate with DPAs in the performance of their tasks and particularly in order to ensure adequate and timely replies to requests received from DPAs. IIJ Business Entities also accept to be audited by 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 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 DPAs on any issues regarding data protection.

8.3. Notifications at the Time of Personal Data Breach

If a Personal Data breach has occurred at an IIJ Business Entity, each IIJ Business Entity's Chief Privacy Office and IIJ Business Entity's CPO shall, in cooperation with the IIJ Chief Privacy Office, IIJ CPO and the DPO, promptly notify the competent DPA to that effect. In order to ensure necessary notification to the relevant parties, the IIJ Business Entities shall follow the procedures in Section 2.6.2.

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

9.1. Data Protection Impact Assessment

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

9.2. Data Protection by Design and by Default

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

9.3. Development of Products and Services

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

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

9.4. Development of New Business and Mergers & Acquisitions

Where an IIJ Business Entity intends to develop new business or to merge with or acquire a company, as of the beginning of these projects, it shall take into account and implement appropriate technical and organisational measures.

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

10. [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.]

17. [This section is not public.]

18. [This section is not public.]

19. [This section is not public.]

20. [This section is not public.]

END

Supplementary Provisions

The IIJ BCR-C are enacted from 28th July 2021.