DATA PROCESSING AGREEMENT

1. General

1.1 Siemens Industry Software Inc., or one of its Siemens Industry Software affiliated companies (collectively referred to herein as "**SISW**") has entered into a cloud services agreement with a customer that has signified its acceptance of the terms and conditions of the cloud services agreement (the "**Customer**"), which may have taken the form of a written agreement signed by both parties or a click-wrap or online agreement agreed to by Customer electronically (referred to herein as the "**Agreement**"). This Data Processing Agreement (the "**DPA**") is specific to the Services where SISW processes any Personal Data of data subjects who are in the European Union on behalf of Customer. This DPA is entered into between SISW and the Customer. SISW retains the right to utilize its affiliated companies in pursuing any of its rights and fulfilling any of its obligations under this DPA. Therefore, the term "SISW" as used herein may also refer to affiliated companies that are directly or indirectly owned or controlled by the ultimate parent company of Siemens Industry Software Inc. and who have been authorized by Siemens Industry Software Inc. to distribute SISW cloud services.

1.2 This DPA is additional to the terms in the Agreement and, to the extent that the terms in this DPA are in conflict with the terms of the Agreement, the terms in this DPA will take precedence and supersede the terms of the Agreement. With respect to any Services that are cloud services, the terms in this DPA will take precedence and supersede the SISW "General Data Protection Terms" incorporated in the Agreement.

1.3 Capitalized terms shall have the meaning given to them above or in Section 12 and otherwise shall have the meaning given to them in the Agreement.

2. Purpose and Scope

2.1 This DPA serves as written commissioned data processing agreement between Customer and SISW and applies to the Services. The DPA constitutes Customer's and SISW's data protection related rights and obligations with regard to the Services. All other rights and obligations shall be exclusively governed by the other parts of the Agreement.

2.2 In providing the Services, SISW shall observe all data protection laws and regulations directly applicable to Processors and shall Process Personal Data only in accordance with the terms of the Agreement (including this DPA). Customer shall be responsible for compliance with any laws and regulations applicable to Customer (especially laws and regulations applicable to Controllers) and shall ensure that SISW and its Sub-Processors are allowed to provide the Services as Processor or Sub-Processor.

3. Details of the Processing Conducted by SISW

3.1 The details of the Processing operations conducted by SISW, including the scope, the nature and purpose of the Processing, the types of Personal Data Processed and the categories of affected data subjects, are specified in Attachment 1 provided that the parties may provide further details for a particular Service in an LSDA, SOW or other agreed transaction document.

3.2 Customer acknowledges that the Services are not intended for the Processing of special categories of Personal Data and Customer shall not transfer directly or indirectly any such sensitive data to SISW.

4. Instruction Rights

4.1 As Processor, SISW shall only Process Personal Data upon Customer's documented instructions. The Agreement (including this DPA) constitutes Customer's complete and final instructions for the Processing of Personal Data by SISW as Customer's Processor. Any additional or alternate instructions must be agreed between SISW and Customer in writing and may be subject to additional costs. SISW shall inform Customer if, in the opinion of SISW, an instruction infringes Applicable Data Protection Law. SISW shall, however, not be obligated to perform any legal examination of Customer's instructions.

4.2 SISW shall, at its own discretion, either (i) provide Customer with the ability to rectify or erase Personal Data via the functionalities of the Services, or (ii) rectify or erase Personal Data as instructed by Customer.

4.3 SISW shall be entitled to disclose or to entitle its Sub-Processors to disclose Personal Data to comply with applicable laws and/or governmental orders. In case of such a request, SISW or the Sub-Processor will (i) redirect such requesting entity to request data directly from Customer and may provide Customer's basic contact information, and (ii) promptly notify Customer and provide a copy of the request, unless SISW is prevented from doing so by applicable laws or governmental order.

5. Technical and Organizational Measures

5.1 SISW shall implement the Measures described in Attachment 2. Customer hereby confirms that the level of security provided is appropriate to the risk inherent with the Processing by SISW on behalf of Customer.

5.2 Customer understands and agrees that the Measures are subject to technical progress and development. In that regard, SISW shall have the right to implement adequate alternative measures as long as the security level of the measures is maintained.

6. Commitment to Confidentiality

6.1 SISW shall ensure that personnel engaged in providing the Services shall maintain the confidentiality of Personal Data.

7. Sub-Processors

7.1 Customer hereby approves the engagement of any affiliates of SISW and any other Sub-Processors contained in Attachment 3 and any additional Sub-Processors may be agreed in accordance with Section 3.1 in any LSDA, SOW or other transactional document.

7.2 SISW shall be authorized to remove or add new Sub-Processors at any time. In such case, new Sub-Processors shall be approved by Customer (such approval not to be unreasonably withheld or delayed) in accordance with the following process:

(i) SISW shall notify Customer with at least ten (10) days' prior notice before authorizing any new Sub-Processors to access Customer's Personal Data;

(ii) if Customer raises no reasonable objections with SISW in writing within this ten (10) day period, then this shall be taken as an approval of the new Sub-Processors, provided SISW informed Customer in the notification about such consequence;

(iii) if Customer raises reasonable objections vis à vis SISW, then SISW shall have the right to terminate the relevant Services with ten (10) days' notice unless SISW chooses in its discretion to (a) continue the Service without the engagement of the Sub-Processor which Customer objected to or (b) take sufficient steps to address the concerns raised in Customer's objection.

7.3 SISW shall be entitled to perform Emergency Replacements of Sub-Processors. In such case SISW shall inform Customer of the Emergency Replacement without undue delay and the process as described in Section 7.2 shall apply mutatis mutandis after Customer's receipt of the notification.

7.4 SISW shall remain fully liable to Customer for the performance of the Sub-Processor's obligations. However, SISW shall not be liable for damages and claims that ensue from Customer's instructions to Sub-Processors.

8. Non-EEA and Privacy Shield Certified Sub-Processors

8.1 In case Transfers to Non-EEA Sub-Processors relate to Personal Data originating from a Controller located within the EEA or Switzerland, this Section 8 shall apply and SISW shall implement the Transfer Safeguards identified per Sub-Processor in Attachment 3 or the respective LSDA, SOW or other transactional document agreed in accordance with Section 3.1. It is Customer's responsibility to assess whether the respective Transfer Safeguard implemented suffices for Customer and Further Service Recipients (if any) to comply with Applicable Data Protection Law.

8.2 If a Transfer Safeguard is based on the EU Model Contract, SISW shall enter into such EU Model Contract with the relevant Sub-Processor. Each EU Model Contract shall contain the right for Customer and Further Service Recipients (if any) located within the EEA or Switzerland to accede to the EU Model Contact. Customer hereby accedes to the EU Model Contracts (as a data exporter) with current Sub-Processors and agrees that its approval of future Sub-Processors in accordance with Section 7.2 shall be deemed as declaration of accession to the EU Model Contact with the relevant future Sub-Processor. Furthermore, Customer agrees to procure that each Further Service Recipient will accede to such EU Model Contract. SISW hereby waives (also on behalf of the respective Sub-Processor) the need to be notified of the declaration of accession of Customer or Further Service Recipients.

8.3 The following shall apply if a Transfer Safeguard is based on the Privacy Shield or Processor Binding Corporate Rules: SISW shall contractually bind such Sub-Processor to comply - as the case may be - with the principles of its Privacy Shield certification or its Processor Binding Corporate Rules.

9. Notification Obligations and SISW Support

9.1 After having become aware of it, SISW shall notify Customer of any Personal Data Breach without undue delay. SISW shall (i) reasonably cooperate with Customer in the investigation of such Personal Data Breach; (ii) provide reasonable support in assisting in Customer in its security breach notification obligations under Applicable Data Protection Law (if applicable); and (iii) initiate respective and reasonable remedy measures.

9.2 SISW shall notify Customer without undue delay of (i) complaints or requests of data subjects whose Personal Data is Processed pursuant to this DPA or (ii) orders or requests by a competent supervisory authority or court.

9.3 At Customer's request and at the Customer's reasonable expense on a time and materials basis, SISW shall reasonably support Customer in (i) dealing with complaints, requests or orders described in Section 9.2 or (ii) fulfilling any of Customer's further obligations as Controller under Applicable Data Protection Law.

10. Audits

10.1 Customer shall have the right to audit, in accordance with Sections 10.2 to 10.4 below – SISW's and Sub-Processors' compliance with the data protection obligations hereunder annually (in particular in regard to the Measures implemented), unless additional audits are necessary under applicable data protection law; such audit being limited to information and data processing systems that are relevant for the provision of the Services provided to Customer.

10.2 SISW and Sub-Processors may use (internal or external) auditors to perform audits to verify compliance with the data protection obligations hereunder. In such case each audit may result in the generation of an audit report. Where a control standard and framework implemented by SISW or our Sub-Processors provides for audits, such audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. Upon Customer's request, SISW shall provide any relevant information in connection with its data protection obligations from such audit reports and corresponding information (together "**Audit Reports**") for the Services concerned.

10.3 Customer agrees that these audit reports shall first be used to address Customer's audit rights under this DPA. In case Customer can demonstrate that the Audit Reports provided are not reasonably sufficient to allow Customer or a Further Service Recipient to comply with the applicable audit requirements and obligations under applicable data protection law, Customer or Further Service Recipient shall specify the further information, documentation or support required. SISW shall render such information, documentation or support within a reasonable period of time at Customer's expense.

10.4 The Audit Reports and any further information and documentation provided during an audit shall constitute SISW Confidential Information and may only be provided to Further Service Recipients pursuant to confidentiality obligations substantially equivalent to the confidentiality obligations contained elsewhere in the Agreement. In case audits relate to Sub-Processors, Customer and Further Service Recipients may be required to enter into non-disclosure agreements directly with the respective Sub-Processor before issuing Audit Reports to Customer or Further Service Recipients.

11. Termination

11.1 Upon termination of the Services, unless otherwise agreed between the Parties, SISW shall erase all Personal Data made available to SISW or obtained or generated by SISW on behalf of Customer in connection with the Services, unless required to retain in accordance with applicable law. The erasure shall be confirmed by SISW in writing upon request.

12. Definitions

12.1 "**Adequacy Decision**" means a decision by the European Commission that a country ensures an adequate level of protection with respect to Personal Data.

12.2 "**Applicable Data Protection Law**" means all applicable law pertaining to the Processing of Personal Data hereunder.

12.3 "**Controller**" means the Customer and – as the case may be – Further Service Recipients which, alone or jointly with others, determine the purposes and means of the Processing of Personal Data.

12.4 "**EEA**" means the European Economic Area.

12.5 "**Emergency Replacement**" refers to a short-term replacement of a Sub-Processor which is necessary (i) due to an event outside of SISW's reasonable control and (ii) in order to provide the Services without interruptions (such as if the Sub-Processor unexpectedly ceases business, abruptly discontinues services to SISW, or breaches its contractual duties owed to SISW).

12.6 "**EU Model Contract**" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established In Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 or any successor agreement issued by the European Commission.

12.7 "**Further Service Recipient**" means any third party (such as an affiliated company of Customer) which is entitled to receive Services under the terms of the Agreement.

12.8 "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

12.9 "**Measures**" means the technical and organizational measures for the protection of Personal Data.

12.10 "**Personal Data**" has the meaning given to that term in the Applicable Data Protection Law and, for the purposes of this DPA, includes only such Personal Data Processed by SISW as Customer's and/or Further Service Recipient's Processor.

12.11 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed under the terms of this DPA.

12.12 "**Processor**" means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of a Controller.

12.13 "**Processor Binding Corporate Rules for Processors**" or "**BCR-P**" means binding corporate rules in the meaning of Section 47 GDPR implemented in a group of companies that apply to Personal Data received from a Controller established in the EEA which is not a member of the group and then processed by the group members as Processors and/or Sub-Processors.

12.14 "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

12.15 "**Privacy Shield**" means – with regard to Controllers located within the EEA – the European Union / United States Privacy Shield arrangement or – with regard to Controllers located in Switzerland – the Switzerland / United States Privacy Shield arrangement.

12.16 "**Services**" means the services (as further specified in an LSDA, SOW or other agreed transaction document) provided under the Agreement that involve the Processing of Personal Data by SISW acting in its role as Processor.

12.17 "**Sub-Processor**" means any further Processor engaged in the performance of the Services provided under the terms of this DPA. Sub-Processor shall only mean a subcontractor with access to Personal Data, a subcontractor without access to Personal Data shall not qualify as Sub-Processor in the meaning of this DPA.

12.18 "**Transfer Safeguards**" means (i) an Adequacy Decision or (ii) appropriate safeguards as required by Section 46 GDPR.

12.19 **"Transfers to Non-EEA Processors**" means (i) the Processing of Personal Data outside the EEA (excluding a country with an Adequacy Decision) or (ii) any accesses to Personal Data from outside the EEA (excluding a country with an Adequacy Decision) by SISW or any of its Sub-Processors.

Attachment 1
Description of the Processing Operations

Data subjects

Unless expressly specified in writing by Customer in an LSDA, SOW or other agreed transaction document, the Personal Data Processed may concern the following categories of data subjects:

(i) end users authorized by Customer to use the Service;

(ii) other personnel of Customer whose Personal Data is stored in the Service; and

(iii) other individuals whose Personal Data is subject to Processing.

Categories of data

Subject to Section 3.2 of this DPA, the Customer shall determine the categories of Personal Data that will be subject to the Processing in connection with the Services. Specific data categories to be stored in the Service are subject to significant configuration by Customer, however some common categories of Personal Data that may be stored in the Service and be subject to the Processing include the following:

(i) name, email address, company name, telephone number, work location, nationality or citizenship, and information regarding access to and use of the Service;

(ii) depending on Customer's configuration of the Service, many other data categories of Personal Data could be present in Customer Data; and

(ii) any other Personal Data that the Customer may provide in connection with the Services.

Processing operations

In providing the Services, SISW may Process Personal Data when performing the following operations as part of the normal operation of the Service, depending on Customer's configuration:

(i) storage and/or archiving on the computing infrastructure maintained by Customer and/or an affiliate company of Customer based in the EU, in single-tenant or multi-tenant environments;

(ii) access or transmission according to instructions issued to the Service by an end user authorized by Customer to use the Service; and

(iii) as part of Service maintenance operations performed by Customer and/or an affiliate company of Customer based in the EU.

Attachment 2
Technical and organizational Measures pursuant to Art. 32 GDPR

1. Introduction
This document describes the Measures which SISW shall implement as a minimum in connection with the Processing of Personal Data carried out by SISW, taking into account the state of the art in technology, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

If different, special measures are agreed in the LSDA, SOW or other agreed transaction document, those special measures apply instead of or in addition to the Measures.

2. Physical Access Control. Unauthorized persons will be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located which Process and/or use the Personal Data.

Measures: All data centers adhere to strict security procedures enforced by security personnel, surveillance equipment, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To ensure proper functionality, physical security equipment (e.g. motion sensors, cameras, etc.) are maintained on a regular basis. In detail, the following physical security measures are implemented at all data centers:

a. In general, buildings are secured through access control systems (smart card access system).
b. Authorization credentials, which include an electronic access badge (unique to the employee, vendor, or contractor) and PIN—are provided to authorized personnel in order to physically access the data center facilities.
c. Physical access to the data centers within the system boundary is enforced by an electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress.
d. Depending on the security classification, buildings, individual areas and surrounding premises are further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
e. Access rights will be granted to authorized personnel on an individual basis according to the System and Data Access Control measures set out below. This also applies to visitor access. Guests and visitors to SISW buildings must register their names at reception and must be accompanied by authorized SISW personnel. SISW and all third party data center providers are logging the names and times of persons entering the private areas of SISW within the data centers.
f. SISW employees and external personnel must wear their ID cards at all SISW locations.

3. System Access Control. Data processing systems used to provide the Service must be prevented from being used without authorization.

Measures:

a. Multiple authorization levels are used to grant access to sensitive systems including those storing and Processing the Personal Data. Processes are in place to ensure that only authorized users have the appropriate authorization to add, delete, or modify users.
b. All users access SISW's systems with a unique user name and a password that must meet certain minimum complexity criteria.
c. SISW and its Sub-Processors have procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If an SISW user changes roles or leaves the company, a process is performed to revoke access rights to the environment.
d. SISW and Sub-Processors have established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, requires regular changes to all user passwords, and requires default passwords to be changed. Personalized user IDs are assigned for authentication. All passwords must meet minimum complexity requirements and are stored in encrypted form. In case of domain passwords, the system forces a password change every 60 days that complies with the minimum complexity requirements. Each SISW computer has a password-protected screensaver.
e. SISW or its Sub-Processors automatically audit the following account events: creation, modification, enabling, disabling, and removal. A system administrator reviews the logs periodically. In the case where the Customer has user creation permission the customer is responsible.
f. Networks of SISW and its Sub-Processors are protected from the public internet by firewalls.
g. SISW and its Sub-Processors use up–to-date antivirus software at access points to the company network, for e- mail accounts, and on all file servers and all workstations.

h. SISW and its Sub-Processors implement security patch management to ensure deployment of relevant security updates.
i. Full remote access to SISW's corporate network and critical infrastructure is protected by strong, multi-factor authentication.

4. Data Access Control. Personnel entitled to use data processing systems will gain access only to the Personal Data that they have a right to access, and the Personal Data must not be read, copied, modified or removed without authorization in the course of Processing, use and storage.

Measures:
a. Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. SISW uses authorization concepts that document how authorizations are assigned and which authorizations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the SISW security policies and standards.
b. All production servers of any SISW Service are operated in the relevant data centers. Security measures that protect applications Processing personal, confidential or other sensitive information are regularly checked.
c. SISW does not allow the installation of personal software or other software not approved by SISW to systems being used for any Service.
d. Should there be a requirement to transfer data due to the failure of underlying data storage media, upon completion of such transfer, the failed storage media will either be degaussed (for magnetic storage) or shredded (for solid-state or optical storage).

5. Data Transmission Control. Personal data must not be read, copied, modified or removed without authorization during transfer.

Measures:
a. The infrastructure and configuration includes network-based intrusion prevention systems (NIPS) and firewalls at system boundaries to protect against malicious communications at the external boundary of the infrastructure. NIPS and firewalls are configured per DISA STIG standards. Data is encrypted in transit using cryptographic modules that comply with FIPS 140-2.
b. Where data carriers are physically transported, adequate measures are implemented at SISW to ensure the agreed service levels (for example, encryption, and lead-lined containers).
c. Transmission of the Personal Data over SISW internal networks is protected in the same manner as any other confidential data according to SISW's security policies.
d. When the data is transferred between SISW and Customer, the protection measures for the transferred Personal Data are as set forth in the Agreement or the relevant documentation for the Service. This applies to both physical and network-based data transfer. Customer assumes responsibility for any data transfer from SISW's Point of Demarcation (e.g. outgoing firewall of the data center which hosts the Service).

6. Data Input Control. The Service will permit retrospective determination whether and by whom Personal Data has been entered, modified or removed from the infrastructure used to provide the Service.

Measures:
a. SISW only allows authorized personnel to access the Personal Data as required in the course of their work. SISW implemented a logging system for input, modification and deletion, or blocking of Personal Data by SISW or its Sub-Processors to the greatest extent supported by the Service.
b. Audit trails provide sufficient detail required to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected. Each operating system event log record includes the event type, a time stamp, the event source, the event location, the outcome of the event, and the user associated with the event.

7. Job Control. Personal Data will be Processed solely in accordance with the terms of the Agreement and any related instructions provided by Customer.

Measures:
a. SISW uses controls and processes to ensure compliance with contracts between SISW and its customers, Sub-Processors, or other service providers.
b. Customer Data will be subject to at least the same protection level as confidential information according to the SISW Information Classification standard.
c. All SISW employees and contractual partners are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SISW customers and partners.

8. Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:
a. SISW employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
b. SISW relies on global cloud service providers to ensure power availability to data centers.
c. SISW has defined contingency plans as well as business and disaster recovery strategies for Services.

9. Data Separation Control. Personal Data collected for different purposes can be Processed separately.

Measures:
a. When applicable, SISW uses the technical capabilities of the deployed software (for example: multi-tenancy or separate system landscapes) to achieve data separation between Personal Data of Customer and that of any other customer.
b. SISW maintains dedicated instances (with logical or physical separation) for each customer.
c. Customer (including its Affiliates) has access only to its own customer instance(s).

10. Data Integrity Control. Ensures that the Personal Data will remain intact, complete, and current during Processing activities:

Measures: SISW has implemented a defense strategy in several layers as a protection against unauthorized modifications. This refers to controls as stated in the control and measure sections as described above. The configuration of firewalls will result in multiple network segments that separate public and private access. Each firewall rule set will have specific access controls specifying the allowed communications between these segments.
a. Security Monitoring Center: Automated intrusion detection software will be used in conjunction with other security prevention and forensics software and process to alert, investigate and if required, notify and assist in the remediation of any security incident.
b. Antivirus software: all systems will have current antivirus definitions configured to protect against virus, worms, trojans, and other forms of malware.
c. Backup and recovery: all systems will have a base level of backup snapshots of data and configuration. If applicable, SISW and its Sub-Processors will also operate a customer's instance with high availability configuration that will ensure that data is stored in two separate data centers of sufficient distance from each other.
d. Regular external audits to prove security measures. SISW and its Sub-Processors will undergo periodic external audits to test the security measures listed above.

Attachment 3 to the Data Processing Agreement
List of approved Sub-Processors

This document lists the Sub-Processors SISW engages when providing Services to Customer.

Sub-Processor Name	Sub-Processor Address	Service provided by Sub-Processor	Transfer Safeguards implemented by Sub-Processor
Smartronix, Inc.	44150 Smartronix Way, Hollywood, Maryland 20636	Managed cloud services	☐Not applicable, Sub-Processor located within the EEA / a Country With An Adequacy Decision ☒EU Model Contract ☐Privacy Shield ☐BCR-P
Amazon Web Services, Inc.	Amazon.com, Inc., 2021 Seventh Ave, Seattle, WA 98121	Cloud services	☐Not applicable, Sub-Processor located within the EEA / a Country With An Adequacy Decision ☐EU Model Contract ☒Privacy Shield ☐BCR-P
Siemens Industry Software (India) Private Limited	Tower C, Panchshil Business Park, Cummins India Office Campus, Survey No. 21, Pune, Balewadi, 411057	Cloud services	☐Not applicable, Sub-Processor located within the EEA / a Country With An Adequacy Decision ☒EU Model Contract ☐Privacy Shield ☐BCR-P
Siemens Product Lifecycle Management Software Inc.	5800 Granite Parkway, Suite 600, Plano, Texas 75024	Cloud services	☐Not applicable, Sub-Processor located within the EEA / a Country With An Adequacy Decision ☒EU Model Contract ☐Privacy Shield ☐BCR-P