FUJITSU

Fujitsu Enterprise Postgres Support Terms and Conditions for Red Hat Marketplace

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SUPPLIER WILL PROVIDE THE SUPPORT SERVICES TO CUSTOMER ONLY IF CUSTOMER FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY USING THE SOFTWARE, CUSTOMER AGREE TO THESE TERMS.

Supplier will use commercially reasonable efforts to respond to the Support Call from the Pre-Registered Contacts for the Software used according to Customer's environment during the Support Period, provided Customer have fully prepaid the annual subscription fees of applicable the Software as defined in the Fujitsu Annual Subscription Agreement provided separately.

The term "Supplier" hereunder shall mean who sells and provides the Support to Customer.

1 Definitions

1.1. "Documentation" means documentations including Read Me files contained in the Software.

1.2. "Error" shall mean a failure of the Software to materially conform to the specifications as described in the applicable Documentation.

1.3. "Initial Response Time" shall mean the target for the elapsed period measured from the time that Customer raises a Support Call until Supplier provides a response which is Supplier's acknowledgment of a Support Call received from Customer.

1.4. "Pre-Registered Contact" shall mean the designated five persons by Customer to be the primary contact points who will submit a notice of technical incidents from Customer to Supplier.

1.5. "Software" shall mean a software defined in the purchase agreement or purchase order form.

1.6. "Support" shall mean the support service provided by Supplier as more specifically described in Section 2.

1.7. "Support Call" shall mean a notice of technical incidents from the Pre-Registered Contact to Supplier via the designated method to contact including web based support system.

1.8. "Support Period" shall mean the subscription period of applicable Software as defined in Fujitsu Annual Subscription Agreement unless otherwise agreed separately in writing.

1.9. "Target Resolution Time" shall mean the target for Supplier of the time required to provide a documented fix that restores full or near full functionality to Customer. This documented fix includes Workarounds. This time shall not include the time delay arising from the time which Supplier waits for Customer's response.

1.10. "Workaround" is a resolution focusing on operational procedures concerning the use of the Software as a result of which Customer can avoid the adverse effects of an Error in the Software without severely compromising the performance of the Software or the integrity of the system or data which operates in conjunction with the Software.

2 Support

2.1 Support

Supplier will use commercially reasonable efforts to provide the followings for applicable Software as the Support during the Support Days and Hours set forth in 2.4 of Section 2:

- a Response to the Support Call to the Pre-Registered Contact;
- the notifications of patch release, failures and security information;
- upgraded version of the Software upon Customer's request with the conditions defined in Fujitsu Annual Subscription Agreement provided separately.

2.2 Customer's responsibilities

Customer will provide the followings to Supplier before the Support Call or until the Support Call is confirmed as closed:

- identify incidents related to the Software;
- isolate and identify problems;
- provide necessary assistance and information reasonably required to solve problems.

Customer is responsible for ensuring the protection of any data containing sensitive, confidential or personal information, including obscuring the logs or otherwise safeguarding such information prior to sending it to Supplier.

Customer acknowledges that Supplier may provide such information to Supplier's subcontractors to solve such problems.

2.3 Support Exclusions

Supplier will not provide the Support in any of the following circumstances:

- An Error and/or inquiry of hardware, network, cloud platform, equipment or software programs other than the Software.
- An Error and/or inquiry from Open Source Software which is not defined in the Documentation of the Software.
- Customer's failure to comply with operating instructions contained in the Documentation.
- Failure to comply with the terms and conditions defined in Fujitsu Annual Subscription Agreement.
- A modification, enhancement or customization of the Software.
- Any cause or causes beyond the reasonable control of Supplier (e.g. floods, fires, loss of electricity, network or other utilities).
- Errors and/or inquiry related to the Software where the applicable support fee is not paid to Supplier.
- An Error and/or inquiry about installation, configuration, management and operation of Customer's applications
- Any professional service requests including, but not limited to performance tuning, advices on design and assistance to installation.
- APIs interfaces or data formats other than those included with the Software
- The Support through access to customer environments remotely/physically.
- The Support call from other contacts than the Pre-Registered Contacts. Supplier will not provide the Support to other contacts than the Pre-Registered Contacts including, but not limited to, Customer's partner and end customers.

2.4 **Support Level**

	Severity 1	Severity 2	Severity 3	Severity 4
Initial Response Time	1 hour			
Target Resolution Time	24 hours	48 hours	7 days*	Best efforts / Future version of software
Support Hours	24 hours			
Support Days	Sunday to Saturday			
Language	English			

* It excludes December 30th through January 3rd in Japan.

2.5 **Definitions of Severity level**

Severity	Definition
Severity 1 - Critical	In a production environment, after a problem occurred in which the user business is completely stopped (Example: file corruption, system down), the recovery also fails, and the business cannot be resumed because there is no Workaround acceptable to the user.
Severity 2 - High	The business is resumed by a temporary Workaround after a part of the user's business in the production environment is stopped or a problem that causes a serious failure to the user's business occurs. But, troubles occur frequently and the business is greatly affected since an effective Workaround cannot be found.
Severity 3 - Moderate	The user's business may be fully used in production environment. However, a feature does not work.
Severity 4 - Low	Aesthetics or changes for convenience; no functional implications

3 Warranties

Supplier warrants that: the Support will be performed in a professional and workmanlike manner. For any breach of the foregoing warranties, Customer's sole and exclusive remedy, and Supplier's sole and exclusive obligation, will be for Supplier to re-perform the Support as warranted, as applicable. If Supplier is unable to correct such non-conformance in the Support after a reasonable opportunity, Supplier will refund the subscription fees paid for the non-conformance; provided that these remedies are only available if Supplier receives notice of such breach within ten (10) days from the date of delivery of the Support, as applicable.

4 Limitations of Liability.

In no event that Supplier's liability arising under this agreement exceed the amount of subscription fee paid by Customer for the 12 months period immediately preceding the event giving rise to such liability. Supplier will not be liable to Customer for any consequential, incidental, special, indirect, or exemplary damages, including without limitation lost profits, business, contracts, revenue, goodwill, production, anticipated savings, loss of data, or costs of procurement of substitute goods or services, or, for any claim or demand by Customer, however caused and (to the fullest extent permitted by law) under any theory of liability (including negligence) even if Supplier has been advised of the possibility of such damages. Customer acknowledges that the amounts payable hereunder are based in part on these limitations, and further agree that these limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

5 Personal Data

Personal data provided to Supplier for the purpose of the Support will be processed in accordance with Exhibit A. For the avoidance of doubt, this provision does not exempt Customer from Customer's obligations under the agreements stipulating the details of the Support.

EXHIBIT A

Data Processing Addendum

A. This Data Processing Addendum (the "Data Processing Addendum") is a part of Fujitsu Enterprise Postgres Support Terms and Conditions for Red Hat Marketplace between Supplier and Customer (the "**Agreement**") for the provision of goods and/or services by Supplier or the Supplier Processors to Customer.

B. To the extent that the Agreement already contains obligations relating to:

compliance with laws and change of laws;

data protection;

security; and

confidentiality,

then this Data Processing Addendum supplements such obligations in the Agreement and does not directly replace or release existing obligations. In the event of a conflict or inconsistency between the terms, the terms of this Data Processing Addendum shall prevail to the extent the conflict relates to the subject matter of this Data Processing Addendum.

C. This Data Processing Addendum sets out how Supplier and the Supplier Processors are to perform their obligations in the context of the Applicable Privacy Law.

Supplier and Customer now agree this Data Processing Addendum as set out above and on the following pages which, along with Schedule 1 and all Appendixes thereto, all form part of and are included in this Data Processing Addendum.

SCHEDULE 1: DATA PROCESSING DESCRIPTION AND APPLICABLE TERMS

DATA PROCESSING DESCRIPTION

Subject matter and duration of processing

Processing of the Processed Personal Data as a direct result of the Agreement and for the duration of Support Period as defined in the Agreement.

Nature and purpose of processing

Processing is for the purposes of Supplier meeting its obligations regarding Support as defined in the Agreement to Customer, under the Agreement and in accordance with the Applicable Law.

Types of Processed Personal Data

Personal data provided by Customer for the purposes of the receipt of goods and/or services in accordance with the Agreement.

Approved Supplier Processors

Customer have consented to Supplier's use of the following Supplier Processors for the purpose of providing the Services and in accordance with this Data Processing Addendum:

Fujitsu Technology Solutions Sp. z o.o.,

Fujitsu Services Limited,

Fujitsu Consulting India Private Limited,

Fujitsu Australia Limited,

K.K. Box Japan,

Box, Inc.

Categories of Data Subjects

Data in respect of individual data subjects provided by Customer or obtained or derived by Supplier pursuant to performance of the Agreement being data in respect of data subjects including:

Data subjects that Customer provide to Supplier, including Customer's employees, Customer's representatives.

APPLICABLE TERMS

DEFINED TERMS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for the purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Applicable Law" means any and all applicable provisions of statutes, laws, rules, codes, treaties, ordinances, decisions, directions, injunctions or regulations, including from any court or any regulatory or governmental authority in any jurisdiction which is relevant to the Services and/or the Agreement.

"Applicable Privacy Law(s)" means any Applicable Law on or relating to data protection or data privacy as amended or updated from time to time.

"Data Subject" shall have the meaning as defined under Applicable Privacy Law or if there is no such definition, means the identified or identifiable natural person to whom Personal Data relates.

"Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is someone who 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.

"Personal Data Breach" means

i) a data breach as defined in the Applicable Privacy Law (if any); or

ii) if there is no definition in the Applicable Privacy Law, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Processed Personal Data.

"Processed Personal Data" means Personal Data processed by Supplier and/or any Supplier Processor in the course of i) providing the Services, or ii) otherwise performing obligations under the Agreement.

"Service Recipient" means Customer and/or another person receiving services under the Agreement.

"Services" means the goods or services to be provided under the Agreement.

"Sub-Contractor" means a person (other than an employee) sub-contracted or otherwise used by Supplier (directly or indirectly) to perform services under the Agreement (not necessarily services involving the processing of Personal Data).

"Supplier Processor" means Supplier's Affiliates or Sub-Contractors processing Processed Personal Data in accordance with this Data Processing Addendum.

"Supervisory Authority" means an independent public authority that has jurisdiction over the processing of Personal Data under this Data Processing Addendum or, as the case requires, a government agency or authority that has jurisdiction over the processing of Personal Data under this Data Processing Addendum.

To the extent relevant under Applicable Privacy Law, the terms "processing", "processor" and "controller" shall have the meaning given to them in the Applicable Privacy Law.

1. SUPPLIER OBLIGATIONS

Where the Supplier and/or a Supplier Processor processes Processed Personal Data in the course of providing the Services, or otherwise to perform obligations under the Agreement and/or this Data Processing Addendum for Customer:

1.1 Supplier shall comply with Applicable Privacy Law in relation to the processing of Processed Personal Data;

1.2 the parties acknowledge that, to the extent relevant under the Applicable Privacy Laws, Supplier will act as a processor for Customer as controller;

1.3 Supplier shall align their processing with the Data Processing Description set out in Schedule 1 and any other processing description agreed in writing between the parties which forms part of this Data Processing Addendum;

1.4 Supplier shall only process the Processed Personal Data on the documented instructions of Customer and in accordance with this Data Processing Addendum; and

1.5 Supplier shall ensure that any persons including their employees authorised to process, or otherwise have access to, the Processed Personal Data have committed themselves to confidentiality on appropriate terms and/or are under an appropriate binding legal obligation of confidentiality.

2. CUSTOMER OBLIGATIONS

2.1 Customer warrant, represent and undertake for itself and for any other Service Recipient that (i) Customer and/or such Service Recipient shall comply in all respects with Applicable Privacy Laws; and (ii) all instructions Customer and/or such Service Recipient gives to Supplier regarding Processed Personal Data shall at all times be in accordance with Applicable Privacy Laws.

2.2 Customer and/or any other Service Recipient are responsible for complying with all obligations under Applicable Privacy Law (including any obligations to give notice to and/or obtain consent from individuals whose Personal Data is processed under the Agreement or this Data Processing Addendum) such that Supplier can lawfully process the Processed Personal Data as contemplated by this Data Processing Addendum.

3. TECHNICAL AND ORGANISATIONAL MEASURES

Supplier shall at all times have in place technical and organizational measures to protect the Processed Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Such measures shall be appropriate to the risks of varying likelihood and severity to the rights and freedoms of individuals that arise as a result of the processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing ("**Appropriate**"), including implementing an Appropriate information security program in accordance with the security measures set out in Appendix 1 (Security Requirements).

4. COOPERATION

4.1 Supplier shall give Customer, at Customer's reasonable cost, such co-operation, assistance and information as Customer may reasonably request and Supplier may reasonably be able to provide, taking into account the nature of processing and the

information available to Supplier, and as is necessary to enable Customer to comply with its obligations under Applicable Privacy Laws and co-operate with the Supervisory Authority in relation to the Processed Personal Data, including assisting Customer:

4.1.1 by taking appropriate technical and organisational measures, to respond to requests from Data Subjects for access to or rectification, erasure, portability, or restriction of or objection to processing, of Processed Personal Data; and

4.1.2 in ensuring compliance with Customer's security, data breach notification, impact assessment and Supervisory Authority consultation obligations under Applicable Privacy Laws, taking into account the information available to Supplier.

5. SUBPROCESSING

5.1 Customer agree that Supplier may disclose, transfer, or make accessible the Processed Personal Data to the Supplier Processors for the purpose of providing the Services under the Agreement subject to the following:

5.1.2 Supplier shall maintain a list of the Supplier Processors and the processing activities to be performed in connection with such disclosures;

5.1.2 Supplier shall provide Customer with at least 8 working days' prior notice of the addition of any new Supplier Processor to this list and the opportunity to object to such addition; and

5.1.3 if Customer, acting reasonably, make such an objection on reasonable grounds and Supplier is unable to modify the Services to prevent disclosure of Processed Personal Data to the additional Supplier Processor, Customer and Supplier shall negotiate in good faith to agree an appropriate replacement Supplier Processor.

5.3 Supplier shall ensure that each (if any) Supplier Processor is party to a written contract imposing on it obligations which are (at least) materially equivalent to those imposed on Supplier by this Data Processing Addendum.

5.4 Supplier shall remain responsible for the compliance by any Supplier Processor with the terms of the Applicable Privacy Law and this Data Processing Addendum.

6. DATA SECURITY INCIDENT

6.1 Supplier shall, without undue delay, give written notice to Customer, if it becomes aware of the occurrence of any Personal Data Breach.

6.2 In relation to any Personal Data Breach Supplier shall:

6.2.1 take reasonable steps to identify and mitigate the underlying cause of the Personal Data Breach so as to minimize the risk of its repetition and the occurrence of similar Personal Data Breach;

6.2.2 take such steps as Supplier may consider necessary to mitigate the risk to Data Subjects as a result of the Personal Data Breach; and

6.2.3 on reasonable request from Customer and subject to obligations of confidentiality, make available to Customer information about the Personal Data Breach necessary for Customer to comply with its obligations under Applicable Privacy Law.

7. AUDIT

7.1 Supplier shall make available to Customer all information (including records and written documents) necessary to demonstrate Supplier's compliance with its obligations under Applicable Privacy Law in relation to the Processed Personal Data.

7.2 If Customer are not reasonably satisfied that the information provided to Customer by Supplier reasonably demonstrates Supplier's compliance with its obligations under Applicable Privacy Law in relation to the Processed Personal Data, Supplier shall allow for and contribute to audits, including inspections, conducted by Customer (or its appointed auditor) subject to the following:

7.2.1 Customer shall give Supplier no less than one months prior written notice of any audit or inspection to be conducted and shall ensure that Customer make (and ensure that each of its appointed auditors makes) reasonable endeavors to avoid causing any material impact on Supplier in the course of such an audit or inspection;

7.2.2 the audit shall only be undertaken inside normal business hours (9am – 5pm on a weekday excluding public holidays);

7.2.3 Customer shall undertake no more than one audit in any calendar year, except for any additional audits or inspections which Customer is required or requested to carry out by Applicable Law or a Supervisory Authority; and

7.2.4 Customer (and its appointed auditors) shall not be authorized to access, copy or otherwise process any other Customer's data or Supplier data that is not Processed Personal Data.

7.3 Customer shall ensure that before any audit is undertaken the individual conducting the audit has entered into a confidentiality agreement with Supplier and that the individual is only authorized to access documents or areas of Supplier which are necessary to demonstrate compliance with Applicable Privacy Law.

8. PROCESSING INSTRUCTIONS

8.1 Supplier shall inform Customer (but without any obligation to give legal advice) if, in its opinion, to follow an instruction given by Customer would give rise to a breach of Applicable Privacy Law.

9. INTERNATIONAL DATA TRANSFERS

9.1 Customer agree that Supplier may transfer Processed Personal Data to a country or territory outside the geographical area of Customer. If Supplier transfers Processed Personal Data to a country outside the applicable geographical area, the transfer shall be made in full compliance with all Applicable Law.

The applicable geographical area includes Japan (Fujitsu Limited locates), Poland (Fujitsu Technology Solutions Sp. z o.o. locates), Netherlands, Ireland and the United Kingdom (Fujitsu Services and its server locates), India (Fujitsu Consulting India Private Limited locates), Australia (Fujitsu Australia Limited locates), the United States of America (server of Box service locates)

Europe Specific Provisions

9.2 Customer agree that Supplier may transfer Processed Personal Data out of the European Economic Area and/or the United Kingdom (as applicable), to a country or territory outside that geographical area, subject always to the following conditions:

9.2.1 the transfer must be made in full compliance with all Applicable Law;

9.2.2 without limitation to clause 9.2.1 above, Supplier must:

9.2.2.1 provide appropriate safeguards in relation to the transfer;

9.2.2.2 ensure that the Data Subject has enforceable rights and effective legal remedies;

9.2.2.3 ensure there is an adequate level of protection for any Processed Personal Data transferred in accordance with Applicable Privacy Law; and

9.2.2.4 execute any additional contracts or documentation as is necessary to comply with Applicable Privacy Law.

10. DATA RETURN OR DESTRUCTION

On written request from Customer and in any event promptly following termination or expiry of the Agreement, Supplier shall delete or return to Customer all the Processed Personal Data in its possession or under its control, unless otherwise required by Applicable Law. In the case of return of the data, Supplier shall as soon as is practicable securely delete all other copies of the Processed Personal Data, unless otherwise required by Applicable Law.

11. MISCELLANEOUS

11.1 Governing Law and Jurisdiction: The construction, validity and performance of this Data Processing Addendum and all matters relating to the interpretation and effect of this Data Processing Addendum and non-contractual obligations arising from or connected with this Data Processing Addendum (and any amendment hereto) shall be governed by the laws as stated in the Agreement or if no governing law is stated in the Agreement the laws of England and Wales.

11.2 Invalidity: If any provision of this Data Processing Addendum (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed not to form part of this Data Processing Addendum, and the validity and enforceability of the other provisions of this Data Processing Addendum shall not be affected.

APPENDIX 1: MINIMUM SECURITY REQUIREMENTS

Supplier maintains and enforces the technical and organisational measures as may be set out in the relevant Agreement or agreed in writing between the parties. The following is a description of some of the core technical and organizational security measures implemented by Supplier:

1.1 **Policies and Standards**

- Establish a policy framework of IT security, risk, and compliance management policies and guidelines. Integrate the controls based on appropriate risk assessments and evolving industry standards.
- Have an information security policy describing objectives, responsibilities and mandatory rules for protection of information. This policy should include data security controls such as data classification, physical security controls, encryption and training, among others. As an extension of such Information Security Policy, document the Process, procedures, organizational structures, and software and hardware functions.
- Maintain additional security standards, guidelines, and baselines which set forth further directions for implementation of specific, required controls such as internal firewalls and account and password management, among others.

1.2 **Information Classification and Access Control**

- Treat information required to conduct its business as a corporate asset, which must be protected against loss and infringements on integrity and confidentiality. Each organizational unit should be required by policy to assess risks to information assets and periodically check the level of security through security reviews.
- Information should be classified based on the nature of such information.
- All employees should be assigned unique User-IDs. Only authorized individuals should be able to grant, modify, or revoke access to an information system that uses or houses Personal Information, and access may be granted for valid business purposes only.
- User administration procedures should define user roles and their privileges, how access is granted, changed and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms. Should maintain commercially reasonable physical and electronic security measures to create and protect passwords.

1.3 **System Integrity and Availability**

- Should maintain network security using commercially available equipment and commercially reasonable techniques.
- In the event of degradation or failure of the information infrastructure, should implement appropriate disaster recovery and business resumption plans. Back-up copies of critical business information and software should be created regularly and tested to ensure recovery.
- IT Security Controls should require appropriate logging and monitoring to enable recording of IT security related actions.

1.4 **Virus and Malware Controls**

- Should maintain anti-virus and malware protection software on its system.

1.5 **Security Incidents**

- All personnel should be required to report any observed or suspected Personal Information security incidents in accordance with appropriate incident reporting procedures.

1.6 **Physical Security**

- Should maintain commercially reasonable security systems at all sites at which an information system that uses or houses personal data is located. Secured areas should employ various physical security safeguards, including use of security badges (identity controlled access) and security guards stationed at entry and exit points. Visitors should only be provided access where authorized.

1.7 **Training & Compliance**

- Personnel should be required to read and abide by the IT security policies as a condition of employment.
- Should implement a security awareness program to train personnel about their security and privacy obligations. This program should include training about data privacy and security practices; physical security controls; and security incident reporting.
- Should regularly monitor the implemented security measures and implementation of new security requirements. Compliance with applicable policies and procedures should be accomplished through regular training, periodic reviews of local and organization-wide policies and procedures, and audits.