LOGPOINT DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) applies to Logpoint’s Processing of Personal Data as a Processor on behalf of Logpoint’s customer (“**Customer**”) as part of Logpoint’s provision of Software, Services, or Software-as-a-Service (“**Services**”) to Customer. This DPA forms part of the Master Services Agreement, Terms of Service, End User License Agreement, or other written or electronic agreement (“**Agreement**”) between Logpoint and Customer for the purchase of Services to reflect the parties’ agreement about the Processing of Personal Data.

The provisions of this DPA shall take priority over any similar provisions contained in other agreements between Customer and Logpoint, if the any provisions contradict, directly or indirectly with the provisions of this DPA.

While providing products and/or services to Customer pursuant to this DPA, Logpoint may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

The terms of this DPA will be effective and replace any previously applicable data processing terms as of the date of execution.

Introduction

A. Customer is a Controller of certain Personal Data and wishes to appoint Logpoint as a Processor to Process this Personal Data on its behalf.

B. The parties are entering into this DPA to ensure that Logpoint conducts such data Processing in accordance with Customer's instructions and Applicable Data Protection Law requirements, and with full respect for the fundamental data protection rights of the Data Subjects whose Personal Data will be Processed.

Definitions

In this DPA, the following terms shall have the following meanings:

"**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**" and "**Processing**" (and "**Process**") shall have the meanings given in Applicable Data Protection Law. The term "Personal Data" shall be deemed to include concepts of "Personal information" or "Personally Identifiable Information" if and as those terms may be defined under Applicable Data Protection Law.

"**Applicable Data Protection Law**" shall mean all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU/UK Data Protection Law.

"**EU/UK Data Protection Law**" shall mean: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**") and the Danish Data Protection Act no. 502 af 23/05/2018; (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

“Restricted Transfer" shall mean: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy decision by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

Data Processing

1. *Rights and obligations of Customer (Controller)*. Customer is responsible for ensuring that the Processing of Personal Data takes place in compliance with the Applicable Data Protection Law.

Customer has the right and obligation to make decisions about the purposes and means of the Processing of Personal Data.

Customer shall be responsible, among other, for ensuring that the Processing of Personal Data, which Logpoint is instructed to perform, has a legal basis.

2. *Logpoint (Processor) acts according to instruction*. Logpoint shall Process Personal Data only on documented instructions from Customer, unless required to do so by Applicable Data Protection Law or national law to which Logpoint is subject, in which case Logpoint shall inform Customer of this legal requirement prior to Processing, unless the law concerned prohibits such notification on grounds of important public interests.

Instructions shall be specified in Annex A. Subsequent instructions can also be given by Customer throughout the duration of the Processing of Personal Data, but such instructions shall always be documented and kept in writing, including electronically, in connection with this DPA.

Logpoint shall immediately inform Customer if instructions given by Customer, in the opinion of Logpoint, contravene the Applicable Data Protection Law.

In no event shall Logpoint Process the Personal Data for its own purposes or those of any third party except as set forth in the Agreement. Other than as otherwise agreed upon by the parties in the Agreement or as otherwise permitted under Applicable Data Protection Law, Logpoint shall not (i) sell the Personal Data, or (ii) retain, use or disclose the Personal Data for any commercial purposes.

3. *Confidentiality of Processing*. Logpoint shall ensure that any person that it authorizes to Process the Personal Data (including Logpoint's staff, agents, and subcontractors) (an "**Authorized Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to Process the Personal Data who is not under such a duty of confidentiality.

Logpoint shall ensure that all Authorized Persons Process the Personal Data only as necessary and in accordance to the Customer's instructions. The list of persons who have been granted access shall be kept under periodic review. On the basis of this review, such access to Personal Data can be withdrawn if access is no longer necessary, and Personal Data shall consequently not be accessible anymore to those persons.

Logpoint shall at the request of Customer demonstrate that the concerned persons under Logpoint's authority are subject to the above-mentioned confidentiality.

4. *Security of Processing*. Logpoint shall implement appropriate technical and organizational measures to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data (a "**Security Incident**"). Such measures shall have regard to the state of the art, 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. Such measures may include, as appropriate:

A. the pseudonymization and encryption of Personal Data;
B. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
C. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
D. a Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Logpoint shall also – independently from Customer – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, Customer shall provide Logpoint with all information necessary to identify and evaluate such risks.

Furthermore, Logpoint shall assist Customer in ensuring compliance with Customer's obligations pursuant to Applicable Data Protection Law in regard to obligations related to security of Processing, by inter alia providing Customer with information concerning the technical and organisational measures already implemented by Logpoint pursuant to Applicable Data Protection Law along with all other information necessary for Customer to comply with Customer's obligation under Applicable Data Protection Law.

5. Use of *Sub-Processors*. Logpoint has Customer's general authorization for the engagement of Sub-Processors. Logpoint maintains an up-to-date list of its Sub-Processors at Logpoint List of Sub-processors - Logpoint. By accepting and/or signing this DPA, Customer accepts the use of the listed Sub-Processors.

Logpoint shall inform Customer of any intended changes concerning the addition or replacement of Sub-Processors at least 30 days in advance, thereby giving Customer the opportunity to object to such changes prior to the engagement of the concerned Sub-Processors.

Customer may object to Logpoint's appointment or replacement of a Sub-Processor at any time prior to their appointment, provided such objection is on reasonable grounds relating to the protection of the Personal Data. In such event, Logpoint will either not appoint or replace the Sub-Processor or, if this is not possible, Customer may suspend or terminate this DPA.

Logpoint shall impose data protection terms on any Sub-Processor it appoints that protect the Personal Data to substantially similar terms to the terms of this DPA. Logpoint remains fully liable to Customer for any breach of this DPA that is caused by an act, error or omission of its Sub-Processors.

6. *Restricted Transfers*. Customer authorizes Logpoint to carry out Restricted Transfers of Personal Data provided that the Restricted Transfer shall be subject to the appropriate Standard Contractual Clauses as follows:

a. in relation to Personal Data that is protected by the EU GDPR, the EU SCCs Module three (processor to processor) will apply for Logpoint as the data exporter and Logpoint's Sub-Processor(s) as data importer.

b. in relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

i. for so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of personal data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("**Prior C2P SCCs**") for transfers of personal data from the United Kingdom, the Prior C2P SCCs shall apply between the "Customer" and the Logpoint on the following basis: (aa) Annex I shall be completed with the relevant information set out in Annex I to this DPA; (bb) Annex II shall be completed with the relevant information set out in Annex II to this DPA; and (cc) the optional illustrative indemnification Clause will not apply;

ii. where sub-clause (b)(i) above does not apply, but the "Customer" and the Logpoint are lawfully permitted to rely on the EU SCCs for transfers of personal data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then: (aa) the EU SCCs, completed as set out above in clause 3(a) of this DPA shall also apply to transfers of such Personal Data, subject to sub-clause (bb); and (bb) the UK Addendum shall be deemed executed between the transferring "Customer" and the Logpoint, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data;

iii. If neither sub-clause (b)(i) or sub-clause (b)(ii) applies, then the "Customer" and the Logpoint shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK GDPR without undue delay; and

7. *Cooperation and Data Subjects' Rights*. Logpoint shall provide all reasonable and timely assistance to Customer to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, limitation, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of the Personal Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Logpoint, Logpoint shall promptly inform Customer providing details of the same. Logpoint will not respond to the Data Subject request without instructions from Customer.

8. *Data Protection Impact Assessment*. If Logpoint believes or becomes aware that its Processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform Customer and provide Customer with all such reasonable and timely assistance as Customer may require conducting a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

9. *Security Incidents (breach on Personal Data)*. Upon becoming aware of a Security Incident, Logpoint shall inform Customer without undue delay and shall provide all such timely information and cooperation as Customer may require for Customer to fulfil its data breach reporting obligations, including the obligation to notify the affected Data Subjects, under (and in accordance with the timescales required by) Applicable Data Protection Law. Logpoint shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer apprised of all developments in connection with the Security Incident.

10. *Deletion or Return of Data*. After termination or expiration of the Agreement, or upon Customer’s request, Logpoint shall destroy or return to Customer all Personal Data (including all copies of the Personal Data) in its possession or control (including any Personal Data subcontracted to a third party for Processing). This requirement shall not apply to the extent that Logpoint is required by any EU (or any EU Member State) law to retain some or all the Personal Data, in which event Logpoint shall isolate and protect the Personal Data from any further Processing except to the extent required by such law.

11. *Audit*. Logpoint shall make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Applicable Data Protection Law.

Logpoint shall permit, upon Customer ’s written request, a mutually agreed-upon third party auditor (the “**Auditor**”) to audit Logpoint's compliance with this DPA and shall make available to such third-party auditor all information, systems, and staff necessary for the Auditor to conduct such audit.

Logpoint acknowledges that the Auditor may enter its premises for the purposes of conducting this audit, provided that Customer gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Logpoint's operations.

Customer will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) “Customer” reasonably believes a further audit is necessary due to a Security Incident suffered by Logpoint. The Customer is responsible for the cost of the audit.

Logpoint shall be required to provide the relevant supervisory authorities, which pursuant to Applicable Data Protection Law have access to Customer’s and Logpoint’s facilities, or representatives acting on behalf of such supervisory authorities, with access to Logpoint’s physical facilities on presentation of appropriate identification.

12. *Anonymized data*. Customer acknowledges and agrees that Logpoint may further use Personal Data it processes pursuant to this DPA for the purposes of creating analytical reports and service improvement, provided that Logpoint first anonymize the Personal Data irrevocably such that neither Customer nor any individual data subject is directly identifiable from the data processed for these purposes.

Logpoint and Customer have caused this DPA to be executed by their duly authorized representatives as of the Effective Date.

Customer

____

Signature: ____________________________

Printed Name: __________________________

Title: _______________________________

Data Signed: ___________________________

Logpoint

Signature: ____________________________

Printed Name: __________________________

Title: _______________________________

Data Signed: ___________________________

Annex I
Data Processing Description

Terms used but not defined in this Appendix shall have the meanings given to them in the Logpoint Data Processing Addendum and any Master Services Agreement, Terms of Service, End User License Agreement, or other written or electronic agreement between Logpoint and CUSTOMER for the purchase of Services.

A. LIST OF PARTIES

Controller(s):

1	Name:	Customer. The customer’s details are specified in the Agreement for the Services with Logpoint.
	Address:	As above.
	Contact person’s name, position and contact details:	As above.
	Activities relevant to the data transferred under these Clauses:	Customer has purchased Services from Logpoint pursuant to the Agreement.
	Signature and date:	This Annex I shall be deemed executed upon execution of the DPA.
	Role (controller/processor):	Controller.

Processor:

2	Name:	Each non-EEA and non-UK member of the Logpoint group of companies, details of which can be found at https://www.Logpoint.com/en/sub-processors/
	Address:	As above.
	Contact person’s name, position, and contact details:	Senior Legal Counsel (Privacy) Email: privacy@Logpoint.com
	Activities relevant to the data transferred under these Clauses:	Provision of Services to the Customer pursuant to the Agreement.
	Signature and date:	This Annex I shall be deemed executed upon execution of the DPA.
	Role (controller/processor):	Processor for the Customer.

B. INSTRUCTION AND DESCRIPTION OF THE PROCESSING AND TRANSFER OF PERSONAL DATA

Categories of data subjects whose personal data is processed and transferred:	Customer may submit Personal Data to Logpoint through Services, as applicable, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: - Prospects, Customer's business partners and vendors of Customer (who are natural persons) - Employees or contact persons of Customer prospects, Customer business partners and vendors - Employees, agents, advisors, freelancers of Customer (who are natural persons) - Data Customers Users authorized by Customer to use Logpoint's products and/or services (who are natural persons)
Categories of personal data processed and transferred:	Customer may submit Personal Data to Logpoint through Services, as applicable, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: - First and last name - Title/Position - Contact information (company, email, phone, physical business address) - Network data (including source and destination IP addresses and domains, approximate geolocation based on IP lookup, network traffic flows, communications metadata, machine names, and unique device identifiers) - User and endpoint behavior (including user account activity & metadata, applications executed on endpoints, and accessed URLs) - Application logs (including firewall logs, DHCP/DNS logs, intrusion detection logs, malware logs, cloud service logs, proxy logs, file access logs) - Other relevant machine data which the Customer elects to send to the Logpoint for processing.

Sensitive data processed and transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Not applicable. Logpoint's Services are not intended nor set up for processing of sensitive personal data (special categories of personal data, incl. personal data about criminal matters). The Customer shall not use Logpoint's Services to process sensitive personal data, unless it is specifically agreed with Logpoint, provided that Logpoint receives written instructions from the Customer of this matter.
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous for the duration of the Services.
Nature of the processing:	Processing of Personal Data necessary to provide the Services specified in the Agreement.
Purpose(s) of the data processing and transfer, incl. further processing:	The Personal Data will be processed for the purpose of providing the Services.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	For the duration of the Services and as otherwise specified in the DPA, paragraph 10.
For processing and transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	As specified above in paragraph 5, and in the Agreement and the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance:	Where the EU GDPR applies, the competent supervisory authority shall be the supervisory authority in the specific country that the data exporter is located and established in. If there are more than one supervisory authority in the data exporter's country, the specific supervisory authority must be specified here. Where the UK GDPR applies, the competent supervisory authority shall be the UK Information Commissioner's Office.

Annex II

Technical and Organizational Security Measures

Description of the technical and organizational measures implemented by Logpoint to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymization and encryption of personal data	Data is encrypted in-transit using TLS. Where applicable, data is encrypted at rest within the product(s) by AWS.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Logpoint uses vulnerability assessment, patch management, threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Logpoint uses multiple types of automated vulnerability scans and assessments which are run at various frequencies (e.g. when code changes occur, daily, weekly, and monthly). Additionally, we perform annual third-party penetration tests and industry security audits.
Measures for user identification and authorisation	Logpoint uses logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions (e.g., use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates).
Measures for the protection of data during transmission	Data is encrypted in transit using TLS.
Measures for the protection of data during storage	Where applicable, data is encrypted within the product(s) by AWS.
Measures for ensuring physical security of locations at which personal data are processed	Logpoint maintains physical and environmental security controls of areas, within Logpoint's facilities, containing client confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of Logpoint's facilities, and

	(iii) guard against environmental hazards. Physical security controls such as logged keycard access to buildings and sensitive areas in buildings, fire alarms and suppression systems, are in use. For Logpoint's Insight products hosted in AWS, physical and environmental controls are inherited from AWS.
Measures for ensuring events logging	Logpoint has system audit and event logging and related monitoring procedures in place to record user access and system activity. Automated analytics are used to generate alerts for suspicious or potentially malicious activity.
Measures for ensuring system configuration, including default configuration	Logpoint uses configuration management tools to deploy and enforce baseline configurations on our systems.
Measures for internal IT and IT security governance and management	Logpoint uses network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, as well as intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of an attack. Additionally, Logpoint has Incident/problem management procedures designed to allow Logpoint to investigate, respond to, mitigate, and notify of events related to Logpoint technology and information assets. Change management controls and procedures are established to ensure human review of production changes is performed to identify potential security issues before changes are made.
Measures for certification/assurance of processes and products	Logpoint regularly reviews its processes on an annual or as-needed basis.
Measures for ensuring data minimisation	Logpoint has an Acceptable Use Policy which covers the ways in which personal data may be used, transferred, stored, and deleted. The policy states that personal data "should only be stored on Logpoint technology assets and only the minimum information necessary to satisfy a business need should be stored."
Measures for ensuring data quality	Logpoint uses change management procedures and tracking mechanisms designed to test, approve, and monitor changes to Logpoint and information assets.

Measures for ensuring limited data retention	Data retention policies are in place which comply with applicable laws and are reviewed regularly by information security and applicable stakeholders.
Measures for ensuring accountability	Logpoint has a robust Information Security department which is tasked with ensuring accountability and consists of three groups: Trust & Security Governance, Risk, and Compliance (GRC); Security Operations and Engineering; and Portfolio and Program Management. The Trust & Security GRC group is responsible for security governance (defining and socializing security policies and standards), security risk management (risk assessments, maturity assessments, etc.), security compliance (coordinating audits for third-party compliance assessments), “CUSTOMER” trust (responding to security questionnaires, etc.) and security training and culture. The Security Operations and Engineering group is responsible for network and host-based vulnerability assessments, threat detection, and incident response; cloud security, network security, and endpoint security; and application security. The Portfolio and Program Management group is responsible for providing project management support, coordinating and updating strategic roadmaps, and driving cross-functional alignment processes
Measures for allowing data portability and ensuring erasure	Data subject request processes are in place to handle erasure and data portability requests. “CUSTOMER” s may reach out to privacy@Logpoint.com in order to exercise their rights.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller (and, for transfers from a processor to a sub-processor, to the data exporter).

Measure	Description
Support to fulfil data subjects' rights	As specified in paragraph 7 of the DPA.