

End User Data Processing Agreement for SAP Support and Professional Services

This End User Data Processing Agreement ("End User DPA") applies if User has Hexagon Software Products with SAP Business Objects Software. Capitalized terms not defined herein are defined in the PERSONAL DATA PROCESSING AGREEMENT FOR SAP SUPPORT AND PROFESSIONAL SERVICES ("SAP DPA") attached hereto and made a part of this End User DPA.

Hexagon and SAP have entered into an agreement through which SAP grants Hexagon the right to provide support services to Hexagon's customers ("End Customers").

In accordance with the agreement, SAP will provide certain support services to Hexagon, and on behalf of Hexagon to End Customers, which may include the processing of, and/or access to, Personal Data controlled by End Customers.

Any such processing of Personal Data requires prior entry into a data processing agreement ("DPA") between all parties of the data processing chain: i.e. (i) a DPA between Hexagon and SAP, and (ii) this End User DPA between Hexagon and End Customer.

This End User DPA includes the general principles of data processing in connection with support services provided by SAP. Hexagon is entering into this End-User DPA for Hexagon to use SAP as a sub-processor of Personal Data as follows.

a) To the extent Personal Data controlled by End Customers, whether or not established in the European Economic Area ("EEA"), is processed by SAP and its Subprocessors within the territory of the EEA, Hexagon is entering into End User DPAs with End Customers. End Customers are hereby required Under this End User DPA to enter a DPA with the same terms with other Controllers who have been authorized by End Customer to receive Support Services under Hexagon's Order Documents with End Customer ("End User Agreement"), except for Section 7.2(b)-(c) of the SAP DPA.

b) Regarding Section 7.2 (b)-(c) of the SAP DPA, if Personal Data controlled by End Customers or Other Data Controllers established within the EEA is processed by SAP and its Subprocessors outside of the EEA, then by executing this End-User DPA, End Customers must include it in their DPAs that End Customers or Other Data Controllers accede to the Standard Contractual Clauses between SAP SE and its relevant Non-EU Subprocessors ("Accession Model"). Other Controllers who have been authorized by End Customer to receive support service under the End User Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as End Customer in accordance with this Section.

c) End Customers may request audit reports or may audit SAP as further detailed in Section 5 of the SAP DPA.

PERSONAL DATA PROCESSING AGREEMENT FOR SAP SUPPORT AND PROFESSIONAL SERVICES

1. BACKGROUND

- 1.1 Purpose and Application.** This document (“**DPA**”) is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data provided by Customer and each Data Controller in connection with the performance of the SAP services as set out in the relevant Agreement (“**SAP Service(s)**”) to which is attached the present DPA which may include:
- (a)** SAP Support as defined in the Software License & Support Agreement; and/or
 - (b)** Professional Services as described in the services agreement concluded between SAP and the Customer (“**Services Agreement**”).
- 1.2 Structure.** Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, the categories of data, the data subjects and the applicable technical and organizational measures.
- 1.3 GDPR.** SAP and Customer agree that it is each party’s responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 (“**GDPR**”), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.
- 1.4 Governance.** SAP acts as a Processor and Customer and those entities that it permits to include Personal Data in systems accessible by SAP when performing the SAP Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SAP as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to include Personal Data and it is Customer’s responsibility to forward such information and notices to the relevant Controllers.

2. SECURITY OF PROCESSING

- 2.1 Appropriate Technical and Organizational Measures.** SAP has implemented and will apply the technical and organizational measures set forth in [Appendix 2](#). Customer has reviewed such measures and agrees that the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.
- Appendix 2 applies only to the extent that such SAP Services are performed on or from SAP premises. In the case where SAP is performing SAP Services on the Customer’s premises and SAP is given access to Customer’s systems and data, SAP shall comply with Customer’s reasonable administrative, technical, and physical conditions to protect such data and guard against unauthorized access. In connection with any access to Customer’s system and data, Customer shall be responsible for providing SAP personnel with user authorizations and passwords to access its systems and revoking such authorizations and terminating such access, as Customer deems appropriate from time to time. Customer shall not grant SAP access to Licensee systems or personal information (of Customer or any third party) unless such access is essential for the performance of SAP Services. Customer shall not store any Personal Data in non-production environments.
- 2.2 Changes.** SAP applies the technical and organizational measures set forth in Appendix 2 to SAP’s entire customer base receiving the same SAP Service. SAP may change the measures set out in

Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3. SAP OBLIGATIONS

- 3.1 Instructions from Customer.** SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and Customer may provide further instructions during the performance of the SAP Service. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the performance of the SAP Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted).
- 3.2 Processing on Legal Requirement.** SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.
- 3.3 Personnel.** To process Personal Data, SAP and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.
- 3.4 Cooperation.** At Customer's request, SAP will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data or any Personal Data Breach. SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SAP will correct or remove any Personal Data in SAP's possession (if any), or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.
- 3.5 Personal Data Breach Notification.** SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP.
- 3.6 Data Protection Impact Assessment.** If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as are generally available for the SAP Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA DELETION

Customer hereby instructs SAP to delete the Personal Data remaining with SAP (if any) within a reasonable time period in line with Data Protection Law (not to exceed six months) once Personal Data is no longer required for execution of the Agreement, unless applicable law requires retention.

5. CERTIFICATIONS AND AUDITS

- 5.1 Customer Audit.** Customer or its independent third party auditor reasonably acceptable to SAP (which shall not include any third party auditors who are either a competitor of SAP or not suitably

qualified or independent) may audit SAP's service and support delivery centers and IT security practices relevant to Personal Data processed by SAP only if:

- (a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures through providing a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate). Certifications are available under: <https://www.sap.com/corporate/en/company/quality.html#certificates> or upon request if the certification is not available online; or
- (b) A Personal Data Breach has occurred; or
- (c) An audit is formally requested by Customer's data protection authority; or
- (d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

5.2 Other Controller Audit. Any other Controller may audit SAP's control environment and security practices relevant to Personal Data processed by SAP in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

5.3 Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency, time frame and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited to remote audits where possible. If an on-site audit is mandatory, it shall not exceed one business day. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP.

5.4 Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by SAP of this DPA, then SAP shall bear its own expenses of an audit. If an audit determines that SAP has breached its obligations under the DPA, SAP will promptly remedy the breach at its own cost.

6. SUBPROCESSORS

6.1 Permitted Use. SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

- (a) SAP or SAP SE on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SAP shall be liable for any breaches by the Subprocessor in accordance with the terms of the Agreement;
- (b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA;
- (c) For SAP Support, SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP (under: <https://support.sap.com/en/my-support/subprocessors.html>) or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the SAP Service; and
- (d) For Professional Services, SAP will, upon request of the Customer, make the list available at <https://support.sap.com/en/my-support/subprocessors.html> or identify such subprocessors prior to the start of the applicable SAP Services.

6.2 New Subprocessors. SAP's use of Subprocessors is at its discretion, provided that:

- (a) SAP will inform Customer in advance of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor (i) for SAP

Support - by posting on the SAP Support Portal, or by email, upon Customer's registration on the SAP Portal and (ii) for Professional Services - by similar posting on the SAP Support Portal, or by e-mail, or in other written form;

- (b) Customer may object to such changes as set out in Section 6.3.

6.3 Objections to New Subprocessors.

- (a) SAP Support: If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the SAP Support upon written notice to SAP, such notice to be provided to SAP no later than thirty days from the date SAP informs the Customer of the new Subprocessor. If Customer does not provide SAP with a notice of termination within this thirty days period, Customer is deemed to have accepted the new Subprocessor. Within the thirty days period from the date of SAP informing the Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for providing SAP a notice of termination and does not affect SAP's right to use the new Subprocessor(s) after the thirty days period.
- (b) Professional Services: If Customer has a legitimate reason under Data Protection Law that relates to the Subprocessors' processing of Personal Data, Customer may object to SAP's use of a Subprocessor, by notifying SAP in writing within five business days of SAP's information as per Section 6.2. If Customer objects to the use of the Subprocessor, the parties will come together in good faith to discuss a resolution. SAP may choose to: (i) not use the Subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the Subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the relevant services on five days' written notice. If Customer does not object within five days of receipt of the notice, Customer is deemed to have accepted the Subprocessor. If Customer's objection remains unresolved thirty days after it was raised, and SAP has not received any notice of termination, Customer is deemed to have accepted the Subprocessor.
- (c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.4 Emergency Replacement. SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly.

7. INTERNATIONAL PROCESSING

7.1 Conditions for International Processing. SAP shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

7.2 Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

- (a) SAP and Customer enter into the Standard Contractual Clauses;
- (b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by SAP) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall

- apply if and when SAP has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c) or (d), or a notice to Customer; and/or
- (c) Other Controllers who have been authorized by Customer to include Personal Data under the Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

7.3 Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.4 Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

9. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

9.1 "Authorized Users" means any individual to whom Customer grants access authorization in compliance with a SAP software license to use the SAP Service that is an employee, agent, contractor or representative of (i) the Customer, (ii) Customer's Affiliates, and/or (iii) Customer's and Customer's Affiliates' Business Partners (as defined under the Software License and Support Agreement).

9.2 "Controller" means the 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; for the purposes of this DPA, where Customer acts as Processor for another Controller, it shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

9.3 "Data Protection Law" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by SAP on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

9.4 "Data Subject" means an identified or identifiable natural person as defined by Data Protection Law.

9.5 "Personal Data" means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is supplied to or accessed by SAP or its Subprocessors in order to provide the SAP Service under the Agreement.

9.6 "Personal Data Breach" means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2)

similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

- 9.7 "Professional Services"** means implementation services, consulting services and/or services such as SAP Premium Engagement Support Services, Innovative Business Solutions Development Services, Innovative Business Solutions Development Support Services.
- 9.8 "Processor"** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, be it directly as Processor of a Controller or indirectly as Subprocessor of a Processor which processes Personal Data on behalf of the Controller.
- 9.9 "Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply).
- 9.10 "Subprocessor"** means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP , SAP SE or SAP SE's Affiliates in connection with the SAP Service and which processes Personal Data in accordance with this DPA.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter

The Data Exporter is the Customer who concluded a Software License and Support Agreement and/or Services Agreement with SAP under which it benefits from SAP Service as described under the relevant Agreement. The Data Exporter allows other Controllers to also use the SAP Service, these other Controllers are also Data Exporters.

Data Importer

SAP and its Subprocessors provide the SAP Service as defined under the relevant Agreement concluded by the Data Exporter that includes the following SAP Service:

- Under the Software License and Support Agreement: SAP and/or its Subprocessors provide support when a Customer submits a support ticket because the Software is not available or not working as expected. They answer phone calls and perform basic troubleshooting, and handles support tickets in a tracking system
- under the applicable Services Agreement for Professional Services: SAP and/or its Subprocessors provide Services subject to the Order Form Services and the applicable Scope Document.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, Business Partners or other individuals having Personal Data transmitted to, made available or accessed by the Data Importer.

Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data and/or data fields which could be transferred per SAP Service as stated in the relevant Agreement. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data transferred by Authorized Users and may include financial data such as bank account data, credit or debit card data.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form), if any.

Processing Operations / Purposes

The transferred Personal Data is subject to the basic processing activities as set out in the Agreement which may include:

- use of Personal Data to provide the SAP Service
- storage of Personal Data
- computer processing of Personal Data for data transmission
- execution of instructions of Customer in accordance with the Agreement.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, 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 protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.

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

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy
- All personnel access SAP's systems with a unique identifier (user ID).
- SAP has procedures in place to so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.
- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

- The company network is protected from the public network by firewalls.
- SAP uses up-to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

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

Measures:

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.
- SAP does not allow the installation of software that has not been approved by SAP.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the SAP Services in accordance with the relevant Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at SAP to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
- When data is transferred between SAP and its customers, the protection measures required for data transfer are hereby mutually agreed upon between SAP and its customer and included as a part of the Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems.

Measures:

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the SAP Service to the extent technically possible.

1.6 Job Control. Job Control is required to ensure that personal data processed on behalf of others are processed strictly in compliance with the Customer's instructions

Measures:

SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.

As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.

- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

For SAP Support, SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer system without the knowledge and consent of the customer. For SAP Support, SAP provides a specially designated, secure support ticket facility in which SAP provides a special access-controlled and monitored security area for transferring access data and passwords. SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer on premise system without the knowledge and active participation of the customer.

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

Measures:

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- SAP has defined business continuity plans for business-critical processes;
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.

Measures:

- SAP uses appropriate technical controls to achieve Customer Data separation at all times.
- Customer (including its approved Controllers) will have access only to their own Data based on secure authentication and authorization.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.

Measures:

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

In particular, SAP uses the following to implement the control and measure sections described above.

In particular:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

Appendix 3 to the DPA

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

Article of GDPR	Section of DPA	Click on link to see Section
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(2), 28(3) (d) and 28 (4)	6	SUBPROCESSORS
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application. Structure.
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel.
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(3) (e)	3.4	Cooperation.
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(3) (g)	4	Data Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) (c)	7.2	Standard Contractual Clauses.