HUMANETICS

Data Privacy Terms

Last Modified: August 14, 2024

The Data Privacy Terms ("**DPT**") are agreed between the Humanetics Innovative Solutions Inc. ("**Humanetics**") and the customer ("**Customer**") named in the Agreement.

1. Definitions

1.1. "**Agreement**" means the commercial agreement on the provision of the Offerings between Humanetics and Customer.

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

1.3. "**Binding Corporate Rules for Processors**" or "**BCR-P**" means binding corporate rules for processors which are approved by the competent supervisory authority in the (i) European Union and (ii) the United Kingdom.

1.4. "**Controller**" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.5. "**Country with an Adequacy Decision**" means any country for which the European Commission has decided that such country ensures an adequate level of data protection, and for personal data originating from the UK, any country for which UK adequacy regulations have been made.

1.6. "**Data Subject**" means an identified or identifiable natural person.

1.7. "**DPT**" shall mean this Data Privacy Addendum.

1.8. "**EEA**" shall mean the European Economic Area.

1.9. "**Further Controller**" shall mean any third party (such as an affiliated company of Customer) acting as Controller which is entitled to use or receive Offerings under the terms of the Agreement.

1.10. "**Offerings**" shall mean the Offerings under the Agreement provided by Humanetics acting in its role as Processor. In the Agreement, Offering as defined herein may be referred to as "Service".

1.11. "**Personal Data**" means information that relates, directly or indirectly, to a Data Subject, including without limitation, names, email addresses, postal addresses, identification numbers, location data, online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal Data, for the purposes of the DPT, includes only such Personal Data submitted by or for Customer or any Further Controller to the Offerings or that is accessed by Humanetics in the context of providing the Offerings.

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

1.13. "**Processor**" means a natural or legal person, public authority, agency or any other body which Processes

Personal Data on behalf of a Controller.

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

1.15. **"Restricted Transfer"** shall mean (i) the Processing of Personal Data outside the EEA or a Country with an Adequacy Decision or (ii) any accesses to Personal Data from outside the EEA or a Country with an Adequacy Decision by Humanetics or any of its Subprocessors.

1.16. "**Sensitive Personal Data**" shall mean information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, social security measures, administrative or criminal proceedings and sanctions, or genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

1.17. "**Standard Contractual Clauses**" means the Standard Contractual Clauses EU; and, for Personal Data originating from Controllers located in the United Kingdom, the Standard Contractual Clauses UK.

1.18. "**Standard Contractual Clauses EU**" means the Standard Contractual Clauses (EU) 2021/914 as of 4 June 2021.

1.19. "**Standard Contractual Clauses UK**" means such standard data protection clauses as are adopted from time to time by the UK Information Commissioner's Office in accordance with Applicable Data Protection Law in the UK including, but not limited to, the International Data Transfer Agreement, and the Standard Contractual Clauses EU as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses.

1.20. "**Subprocessor**" shall mean any further Processor engaged by Humanetics that has access to Personal Data.

1.21. "**Transfer Safeguard(s)**" shall mean appropriate safeguards for Restricted Transfers as required by Applicable Data Protection Law, such as appropriate safeguards as required by Article 46 General Data Protection Regulation (EU) 2016/679.

2. SCOPE AND COMPLIANCE WITH LAWS

2.1. The DPT shall apply to the Processing of Personal Data by Humanetics acting as Processor for Customer with respect to Offerings provided under the Agreement.

2.2. The DPT describe Customer's and Humanetics' data protection related rights and obligations with regard to the processing operations captured by the DPT. All other rights and obligations shall be exclusively governed by the terms set forth in the Agreement.

2.3. When providing the Offerings, Humanetics will comply with Applicable Data Protection Laws and regulations directly applicable to its provision of the Offerings acting as Customer's Processor. However, Humanetics shall not be responsible for compliance with any Applicable Data Protection Laws or regulations applicable to Customer or Customer's industry that are not generally applicable to Processors. Customer shall comply with all Applicable Data Protection Laws and regulations applicable to Customer's use of the Offerings, including

Applicable Data Protection Law, and ensure that Humanetics and any Subprocessor are allowed to provide the Offerings as described in the DPT. Customer is solely responsible for ensuring that any Personal Data it provides to Humanetics for processing under the Agreement or this DPT is in compliance with Applicable Data Protection Laws.

3. INSTRUCTIONS

Customer and Humanetics agree that the Agreement, including the DPT, shall function as Customer's documented instructions to Humanetics for the Processing of Personal Data. Any additional or alternative instructions must be agreed to in writing by the parties.

4. TECHNICAL AND ORGANIZATIONAL MATTERS

4.1. Humanetics shall assess the risks associated with the processing of Personal Data and implement the technical and organizational measures set forth in these DPT to appropriately mitigate that risk. Customer understands and agrees that Humanetics may modify and implement alternative technical and organizational measures to accommodate technical progress and development as long as security appropriate security levels are maintained.

4.2. The technical and organizational measures described in Section 18 of these DPT apply to the IT-system and applications of Humanetics and any of its Subprocessors. Customer is responsible for implementing and maintaining appropriate technical and organizational measures for components that Customer provides or controls, such as implementing physical and system access control measures for Customer's own premises, assets and IT-systems or configuring the Offerings to Customer's individual requirements.

5. CONFIDENTIALITY OF PROCESSORS

Humanetics will ensure that personnel who are engaged in the Processing of Personal Data (i) are appropriately trained regarding privacy and security, (ii) are under an obligation to maintain the confidentiality of such data, and (iii) will process such data in accordance with the DPT or other instructions agreed upon by the parties.

6. SUBPROCESSORS

6.1. Customer hereby approves the engagement of Subprocessors by Humanetics. A current list of Subprocessors commissioned by Humanetics is provided in Section 19.

6.2. Humanetics may remove or add new Subprocessors at any time. If required by Applicable Data Protection Law, Humanetics will obtain Customer's approval to engage new Subprocessors in accordance with the following process: (i) Humanetics shall notify Customer with at least 30 days' prior notice before authorizing any new Subprocessor to access Customer's Personal Data; (ii) if Customer raises no reasonable objections that include an explanation of the grounds for non-approval in writing within this 30 day period, then this shall be taken as an approval of the new Subprocessor; (iii) if Customer raises reasonable objections, Humanetics will - before authorizing the Subprocessor to access Personal Data - use reasonable efforts to (a) recommend a change to Customer's configuration or use of the Offerings to avoid Processing of Personal Data by the objected-to new Subprocessor or (b) propose other measures that address the concerns raised in Customer's objection; (iv) if the proposed changes or measures cannot eliminate the grounds for non-approval, Customer may terminate the affected Offering without penalty with 14 days' written notice following Humanetics response to Customer's objection. If Customer does not terminate the affected Offering within the 14-day period, this shall be taken as an approval of the Subprocessor by Customer.

6.3. In case of any commissioning of Subprocessors, Humanetics shall enter into an agreement with such

Subprocessor imposing appropriate contractual obligations on the Subprocessor that are no less protective than the obligations in these DPT. Humanetics remains responsible for any acts or omissions of our Subprocessors in the same manner as for Humanetics' own acts and omissions hereunder.

7. **INTERNATIONAL DATA TRANSFERS**

7.1. Restricted Transfers. In case Restricted Transfers relate to Personal Data originating from a Controller located within the EEA, Switzerland, or the United Kingdom, Humanetics shall implement the Transfer Safeguards identified in these DPT. Humanetics shall have the right to replace the Transfer Safeguard identified in these DPT by alternative adequate Transfer Safeguards. In this case the notification and objection mechanism in Section 6.2 shall apply mutatis mutandis.

7.2. Standard Contractual Clauses. The following shall apply if a Transfer Safeguard is based on the Standard Contractual Clauses:

(a). Option 1 - Humanetics within the EEA. If the Humanetics entity being a party to these DPT is located within the EEA or within a Country with an Adequacy Decision, then this Option 1 shall apply, and the Restricted Transfer shall be protected by Module 3 of the Standard Contractual Clauses EU and the respective provision of the Standard Contractual Clauses UK. Humanetics shall be responsible to conclude the Standard Contractual Clauses covering the relevant Processing activities with its Subprocessors.

(b). Option 2 - Humanetics outside the EEA. If the Humanetics entity being a party to these DPT is located outside the EEA or outside a Country with an Adequacy Decision, then this Option 2 shall apply, and Humanetics and Customer hereby enter into Module 2, and, if the Customer itself acts as Processor for its Authorized Entities, then the parties hereby also enter into Module 3 of the Standard Contractual Clauses EU and the respective provision of the Standard Contractual Clauses UK. For this purpose, the Standard Contractual Clauses available at https://www.humaneticsgroup.com/sw-terms are incorporated in these DPT by reference. Section 16- "Description of the Processing Operations", "Section 18 - Technical and organizational measures" and "Section 19- List of approved Subprocessors" shall form Annex I to III of the Standard Contractual Clauses. Without prejudice to the statutory rights of Data Subjects, limitations of liability contained in the Agreement shall also apply to Humanetics' and its Subprocessors' liability (taken together in the aggregate) vis-à-vis Customer under the Standard Contractual Clauses.

7.3. Onward Transfers. Any further onward transfer must comply with the applicable Module of the Standard Contractual Clauses. In case Customer is located outside the EEA and acts on its part as a data importer for its Further Controllers under the Standard Contractual Clauses, the third-party beneficiary clause stipulated by Clause 9 (e) of the Standard Contractual Clauses shall be in favor of the respective Further Controllers acting as the data exporters under such Standard Contractual Clauses.

7.4. Switzerland. In case Restricted Transfers relate to Personal Data originating from a Controller located within Switzerland and the Standard Contractual Clauses are used, any reference in the Standard Contractual Clauses EU to the EU General Data Protection Regulation (EU) 2016/679 shall be understood as reference to Applicable Data Protection Law in Switzerland and references to the "competent supervisory authority" shall be interpreted as references to the competent data protection authority in Switzerland. The Parties further agree that the Standard Contractual Clauses shall be governed by the laws of Switzerland.

7.5. BCR. The following shall apply if a Transfer Safeguard is based on BCR-P: Humanetics shall contractually bind such Subprocessor to comply with the BCR-P with regard to the Personal Data Processed under the DPT.

8. **DEFEINING CUSTOMER PERSONAL DATA; THIRD-PARTY ACCESS REQUESTS**

In the event Humanetics receives an order from any third party for disclosure of Personal Data, Humanetics shall (i) use every reasonable effort to redirect the third party to request data directly from Customer; (ii) promptly notify Customer, unless prohibited under applicable law, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and, (iii) use all reasonable lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the EEA or applicable EEA member state law

9. **PEERSONAL DATA BREACH**

9.1. Humanetics shall notify the Customer without undue delay after becoming aware of a Personal Data Breach. Taking into account the nature of processing and the information available to Humanetics, the notification shall describe (i) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (ii) a contact point where more information can be obtained, (iii) the likely consequences of the Personal Data Breach; and (iv) the measures taken or proposed to be taken to address the Personal Data Breach. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

9.2. Humanetics shall (i) reasonably assist the Customer in ensuring compliance with its Personal Data Breach obligations pursuant to Applicable Data Protection Law, and (ii) initiate respective and reasonable remedy measures.

10. **DATA SUBJECT RIGHTS; HUMANETICS ASSISTANCE**

10.1. Humanetics shall, to the extent legally permitted, notify Customer without undue delay if Humanetics receives a request from a Data Subject to exercise its Data Subject’s rights (such as the right to access, rectification, erasure or restriction of Processing).

10.2. Taking into account the nature of the processing and the information available to Humanetics , (i) Humanetics shall assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights; (ii) at its own discretion, either (a) provide Customer with the ability to rectify or erase Personal Data via the functionalities of the Offerings, or (ii) rectify or erase Personal Data as instructed by Customer; and (iii) reasonably assist Customer to comply with its further obligations under Applicable Data Protection Law.

11. **AUDITS**

11.1. Provided that an audit right is required by Applicable Data Protection Law, Customer shall have the right to audit, by appropriate means - in accordance with Sections 11.2 to 11.4 below - Humanetics’ and its Subprocessors’ compliance with the data protection obligations hereunder annually, unless additional audits are necessary under Applicable Data Protection Law. Such audits shall be limited to information and data processing systems that are relevant for the provision of the Offerings provided to Customer and such audits shall be carried out at Customer’s cost and expense.

11.2. Humanetics and its Subprocessors may use (internal or external) auditors to perform audits to verify compliance with the data protection obligations hereunder. Each audit will result in the generation of an audit report (“**Audit**

Report”). Upon Customer´s request, Humanetics shall provide such relevant Audit Reports for the Offerings concerned. Customer agrees that these Audit Reports shall first be used to address Customer’s audit rights under these DPT.

11.3. If required under Applicable Data Protection Law, Humanetics will allow for additional audits, including onsite audits at Humanetics facilities and premises by Customer or an independent, accredited third party audit firm, during regular business hours, with reasonable advance notice to Humanetics.

11.4. The Audit Reports and any further information and documentation provided during an audit shall constitute confidential information and may only be provided to Further Controllers pursuant to confidentiality obligations substantially equivalent to the confidentiality obligations contained elsewhere in the Agreement. In case audits relate to Subprocessors, Humanetics may require Customer and Further Controllers to enter into non-disclosure agreements directly with the respective Subprocessor before issuing Audit Reports and any further information or documentation to Customer or Further Controllers.

12. NOTICES

12.1. Humanetics may provide notice to Customer under the DPT by posting a notice as described in the Agreement.

12.2. Notices concerning Subprocessors under Section 6 of the DPT may be given by listing the current Subprocessors at https://www.humaneticsgroup.com/legal-policies and providing Customer with a mechanism to obtain notice of any new Subprocessor. It is Customer’s obligation to register a point of contact to receive Subprocessor notifications at https://www.humaneticsgroup.com/legal-policies and to keep contact information for notices current.

13. TERM AND TERMINATION

The DPT shall have the same term as the Agreement. Upon termination of the DPT and unless otherwise agreed between the parties in the Agreement, Humanetics shall erase all Personal Data made available to it or obtained or generated by it on behalf of Customer connection with the Offerings.

14. LANGUAGE

If Humanetics provides a translation of the English language version of these DPT, the English language version of these DPT will control in the event of any conflict.

15. COUNTRY TERMS

15.1. **Russian Federation.** If Humanetics is Processing Personal Data within the scope of the Data Protection Act No. 152 FZ (i) Customer shall be responsible for the initial collection, recording, systematization, storing, updating, amending, transferring and extraction (collectively “**Initial Processing**”) of such Personal Data; and (ii) Customer hereby represents that it will conduct the Initial Processing in compliance with the laws governing processing and protection of such information. Customer represents that it has obtained the Data Subject’s consent on the transfer (including international transfer) and Processing of their Personal Data by Humanetics and its Subprocessors.

15.2. **USA.** If Humanetics is Processing Personal Data of US residents, Humanetics makes the following additional commitments to Customer: Humanetics will Process Personal Data on behalf of Customer and, not retain, use, or disclose that Personal Data for any purpose other than for the purposes set out in the DPT and as permitted under relevant US data privacy law (“**US Data Privacy Law**“). In no event will Customer sell (as such term is defined under US Data Privacy Law) any such Personal Data. These additional terms do not limit or reduce any data protection commitments Humanetics makes to Customer in the DPT, Agreement, or other agreement between Humanetics and Customer. Humanetics hereby certifies that Humanetics understands the restrictions contained herein and will comply with them.

16. **DESCRIPTIONS OF THE PROCESSING OPERATIONS**

16.1. **List of Processing Parties:**

(a). Customer (and, where the Standard Contractual Clauses apply, data exporter):

(i). **Name, address and contact person's name, position and contact details**: Name and address of the Customer as well as contact details of a contact person are contained in the Agreement and/or collected as part of the Customer onboarding process.

(ii). **Role (Controller/Processor)**: Customer acts as Controller for the processing activities provided by Humanetics vis-à-vis Customer and, as the case may be, as Processor under the instructions of its Further Processors.

(b). Provider (and, where the Standard Contractual Clauses apply, data importer):

(i). **Name, address and contact person's name, position and contact details**: The provider / data importer proving the Processing services hereunder is the Humanetics company specified in the Agreement. Point of contact for data privacy inquiries is the Office of the Humanetics Data Protection Officer, Werner-von-Humanetics -Straße 1, 80333 Munich, Germany, E-Mail:

(ii). **Role (Controller/Processor)**: Humanetics acts as Processor Processing Personal Data on behalf of Customer and, as the case may be, Customer's Further Controllers.

16.2. **Description of Transfer/Processing Operations:**

(a). Categories of data subjects whose Personal Data is transferred/Processed

(i). employees,

(ii). contractors,

(iii). suppliers,

(iv). business partners; and

(v). other individuals whose Personal Data is stored on the Offerings and/or is Processed in the context of providing the Offerings.

(b). The Personal Data transferred/Processed concern the following categories of Personal Data:

(i). contact and user information, including name, address data, phone number, email address, and time zone;

(ii). system access, usage, authorization data, operating data and any system log-files containing Personal Data or any other application- specific data which users enter into the Offerings; and (iii). where applicable further Personal Data as determined by Customer and its Further Controllers by uploading or connecting it to the Offerings or otherwise granting access to it via the Offerings.

16.3. **Sensitive data transferred (if applicable)**: The Offerings are not intended for the processing of Sensitive Personal Data and Customer and its Further Controllers shall not transfer, directly or indirectly, any such Sensitive Personal Data to Humanetics.

16.4. **The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)**:

(a). If the Offering involves the provision of Cloud Services (as specified further below), Humanetics continuously hosts the Personal Data on behalf of the Customer.

(b). If the Offering involves the provision of Support and Professional Offerings (as specified further below), Humanetics may access Personal Data only when providing the respective Offering, unless specified otherwise in the Agreement.

16.5. **Nature of the processing and purpose(s) of the data transfer and further processing:** Humanetics and its Subprocessors will Process Personal Data to provide the Offerings, including:

(i). internet accessible or similar Offerings made available and hosted by Humanetics ("Cloud Offerings"); or

(ii). administration, management, installation, configuration, migration, maintenance and support Offerings or any other Offerings requiring (remote) access to Personal Data stored in the Cloud Offerings or on Customer's IT systems ("Support and Professional Offerings").

16.6. **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** The Personal Data will be retained for the period of the Agreement. Customer has the ability to rectify, erase or restrict the Processing of Personal Data via the functionalities of the services, or (ii) Humanetics rectifies, erases or restricts the Processing of Personal Data as instructed by Customer.

16.7. **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:** The subject matter, nature and duration of the processing are specified per Subprocessor in Section 19.

17. STANDARD CONTRACTUAL CLAUSES: COMPETENT SUPERVISORY AUTHORITY

17.1. Where the Standard Contractual Clauses apply, the supervisory authority responsible for the Customer shall act as competent supervisory authority in the context of the Standard Contractual Clauses. A list of the supervisory authorities in the European Union is available here: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.html

18. **TECHNICAL AND ORGANISATIONAL MEASURES.** This section describes the technical and organizational measures (TOMs) implemented by Humanetics and its Subprocessors to protect Humanetics ' and Subprocessors' IT-systems and applications. Some Offerings may be protected by different or additional TOMs, as set forth in the respective Agreement, including the Offering specific Annexes available at www.Humanetics .com/dpt.

Scenario 1: TOMs applicable to Cloud Offerings.

Scenario 2: TOMs applicable to Support and Professional Offerings provided via remote access tools provided and controlled by Humanetics .

Scenario 3: TOMs applicable to Support and Professional Offerings provided via remote access tools provided and controlled by Customer.

#	Measures	Scenario		
		1	2	3
1.	Physical and Environmental Security			
	Humanetics implements suitable measures to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers and related hardware). This shall be accomplished by:			
	a) establishing security areas;	X	X	-
	b) protecting and restricting access paths;	X	X	-
	c) securing the decentralized data processing equipment and personal computers;	X	X	X
	d) establishing access authorizations for employees and third parties, including the respective documentation;	X	X	-
	e) all access to the data center where Personal Data is hosted will be logged, monitored, and tracked;	X	-	-
	f) the data center where Personal Data is hosted is secured by restricted access controls, and other appropriate security measures; and	X	-	-
	g) maintenance and inspection of supporting equipment in IT areas and data centers shall only be carried out by authorized personnel	X	X	-
2.	Access Control (IT-Systems and/or IT-Application)			
	2.1 Humanetics implements an authorization and authentication framework including, but not limited to, the following elements:			
	a) role-based access controls implemented;	X	X	X
	b) process to create, modify, and delete accounts implemented;	X	X	X
	c) access to IT systems and applications is protected by authentication mechanisms;	X	X	X
	d) appropriate authentication methods are used based on the characteristics and technical options of the IT system or application;	X	X	X
	e) access to IT systems and applications shall require adequate authentication;	X	X	X
	f) all access to data (including personal data) is logged;	X	X	-
	g) authorization and logging measures for inbound and outbound network connections to IT systems and applications (including firewalls to allow or deny inbound network connections) implemented;	X	X	-
	h) privileged access rights to IT systems, applications, and network Offerings are only granted to individuals who need it to accomplish their tasks (least-privilege principle);	X	X	X
	i) privileged access rights to IT systems and applications are documented and kept up to date;	X	X	X
	j) access rights to IT systems and applications are reviewed and updated on regular basis;	X	X	X
	k) password policy implemented, including requirements re. password complexity, minimum length and expiry after adequate period of time, no re-use of recently used passwords;	X	X	X
	l) IT systems and applications technically enforce password policy;	X	X	X
	m) policy to lock user terminal when leaving the workplace;	X	X	X
	n) automatic time-out of user terminal if left idle;	X	X	X
	o) automatic turn-off of the user identification when several erroneous passwords are entered, along with log file of events (monitoring of break-in-attempts);	X	X	X

	p) access rights of employees and external personnel to IT systems and applications is removed immediately upon termination of employment or contract; and	X	X	X
	q) use of secure state-of-the-art authentication certificates.	X	X	-
	2.2 Humanetics implements a roles and responsibilities concept.	X	X	-
	2.3 IT systems and applications lock down automatically or terminate the session after exceeding a reasonable defined idle time limit.	X	X	-
	2.4 Humanetics maintains log-on procedures on IT systems with safeguards against suspicious login activity (e.g. against brute- force and password guessing attacks).	X	X	X
3.	Availability Control			
	3.1 Humanetics defines, documents and implements a backup concept for IT systems, including the following technical and organizational elements:			
	a) backups storage media is protected against unauthorized access and environmental threats (e.g., heat, humidity, fire);	X	-	-
	b) defined backup intervals; and	X	-	-
	c) the restoration of data from backups is tested regularly based on the criticality of the IT system or application.	X	-	-
	3.2 Humanetics stores backups in a physical location different from the location where the productive system is hosted.	X	-	-
	3.3 Humanetics implements state-of-the-art anti-malware solutions to protect its systems and applications against malicious software.	X	X	X
	3.4 IT systems and applications in non-production environments are logically or physically separated from IT systems and applications in production environments.	X	-	-
	3.5 Data centers in which Personal Data is stored or processed are protected against natural disasters, physical attacks or accidents.	X	-	-
	3.6 Supporting equipment in IT areas and data centers, such as cables, electricity, telecommunication facilities, water supply, or air conditioning systems are protected from disruptions and unauthorized manipulation.	X	-	-
4.	Operations Security			
	4.1 Humanetics maintains and implements a company-wide ISO 27001 Information Security Framework which is regularly reviewed and updated.	X	X	X
	4.2 Humanetics logs security-relevant events, such as user management activities (e.g., creation, deletion), failed logons, changes on the security configuration of the system on IT systems and applications.	X	X	X
	4.3 Humanetics continuously analyzes the respective IT systems and applications log data for anomalies, irregularities, indicators of compromise and other suspicious activities.	X	X	X
	4.4 Humanetics scans and tests IT systems and applications for security vulnerabilities on a regular basis.	X	X	X
	4.5 Humanetics implements and maintains a change management process for IT systems and applications.	X	X	X
	4.6 Humanetics maintains a process to update and implement vendor security fixes and updates on the respective IT systems and applications.	X	X	X
	4.7 Humanetics irretrievably erases data or physically destroys the data storage media before disposing or reusing of an IT system.	X	X	X
5.	Transmission Controls			
	5.1 Humanetics continuously and systematically monitors IT systems, applications and relevant network zones to detect malicious and abnormal network activity by;			

	a) Firewalls (e.g., stateful firewalls, application firewalls);	X	X	-
	b) Proxy servers;	X	X	-
	c) Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS);	X	X	-
	d) URL Filtering; and	X	-	-
	e) Security Information and Event Management (SIEM) systems.	X	X	-
	5.2 Humanetics documents and updates network topologies and its security requirements on regular basis.	X	X	-
	5.3 Humanetics administers IT systems and applications by using state-of-the-art encrypted connections.	X	X	-
	5.4 Humanetics protects the integrity of content during transmission by state-of-the-art network protocols, such as TLS.	X	X	-
	5.5 Humanetics encrypts, or enables its customers to encrypt, customer data that is transmitted over public networks.	X	X	-
	5.6 Humanetics uses secure Key Management Systems (KMS) to store secret keys in the cloud.	X	-	-
6.	Security Incidents			
	Humanetics maintains and implements an incident handling process, including but not limited to			
	a) records of security breaches;	X	X	X
	b) customer notification processes; and	X	X	X
	c) an incident response scheme to address the following at time of incident:(i) roles, responsibilities, and communication and contact strategies in the event of a compromise (ii) specific incident response procedures and (iii) coverage and responses of all critical system components.	X	X	X
7.	Asset Management, System Acquisition, Development and Maintenance			
	7.1 Humanetics implements an adequate security patching process that includes:			
	a) monitoring of components for potential weaknesses (CVEs);	X	X	-
	b) priority rating of fix;	X	X	-
	c) timely implementation of the fix; and	X	X	-
	d) download of patches from trustworthy sources.	X	X	-
	7.2 Humanetics identifies and documents information security requirements prior to the development and acquisition of new IT systems and applications as well as before making improvements to existing IT systems and applications.	X	X	-
	7.3 Humanetics establishes a formal process to control and perform changes to developed applications.	X	X	-
	7.4 Humanetics plans and incorporates security tests into the System Development Life Cycle of IT systems and applications.	X	X	-
8.	Human Resource Security			
	8.1 Humanetics implements the following measures in the area of human resources security:			
	a) employees with access to Personal Data are bound by confidentiality obligations; and.	X	X	X
	b) employees with access to Personal Data are trained regularly regarding the Applicable Data Protection Laws and regulations	X	X	X
	8.2 Humanetics implements an offboarding process for Humanetics employees and external vendors.	X	X	X

19. LIST OF APPROVED SUBPROCESSORS

A reference to the Subprocessors used by us when providing the Offering is available at [link to Subprocessor list] or contained in the respective Agreement.

20. **CLOUD OFFERINGS**. This Section 20 sets forth additional terms with respect to Cloud Offerings provided by Humanetics to Customer as set forth in a Cloud SLA or Order pursuant to the Agreement. Unless otherwise set forth herein, capitalized terms in this Section 20 shall have the meanings defined in the Agreement.

20.1. Customer shall be solely responsible for determining the type of data and the individuals affected by the processing and shall ensure the legitimacy of such processing by means of the Cloud Service. Customer shall also be responsible for any correction, deletion or blocking of personal data, using the functionalities offered by the Cloud Service. Customer may export and delete its data, including personal data, using the functionalities offered by the Cloud Service. Upon termination of this Data Processing Agreement, Customer shall have 30 days to send a written request to Humanetics that Customer Data be made available for download by Customer. After expiration of any period set forth by Humanetics in response to such a request, any remaining data of Customer will be subject to deletion and will no longer be available to Customer. Humanetics and Customer agree that, within the scope of the Cloud Service, Customer's right to issue instructions will be exercised exclusively by using the functionalities offered by the Cloud Service. Customer covenants that it will not upload or store any protected health information (PHI) in the Cloud Service

20.2. In providing the Cloud Service, with respect to the production system, Humanetics shall comply with the technical and organizational measures described in Section 18 of these DPT. Non-production systems related to the Cloud Service may or may not comply with the measures described in Section 18 of these DPT. In addition, Humanetics may change the technical and organizational measures applicable to the production system from time to time, provided that such changes do not adversely affect the level of protection afforded by such measures in any material way. Humanetics will restrict its personnel from collecting, processing or using personal data without authorization and will employ only personnel in processing of Customer's personal data which have been specifically instructed in compliance with data privacy protection requirements.

20.3. Humanetics shall be entitled to engage subprocessors in the performance of the Cloud Service as described in this DPT. To the extent access of subprocessors to Customer's personal data cannot be excluded, Humanetics will provide to Customer upon request a list of such subprocessors and their respective locations and will update such list as required before any new subprocessor is granted access to Customer's personal data. In case Customer reasonably objects to any new subprocessor, Customer shall inform Humanetics of such objection and, if Humanetics insists on the engagement of the new subprocessor, shall be entitled to terminate this DPT for good cause. To the extent that engagement of any such subprocessor involves a cross-border transfer of personal data, Humanetics will endeavor to cause such subprocessor to maintain an adequate level of data protection with respect to such personal data.