DATA PROTECTION ADDENDUM ADDRESSING ARTICLE 28 GDPR
For Cloud Services and Related Professional Services

Between
–Customer–

und

Unify Software and Solutions GmbH & Co. KG –
„Unify“ or „Processor“

Table of contents

Preamble

This Data Protection Addendum ("DPA") forms part of the Terms of Service Production for Unify Phone Service (hereinafter "Customer Agreement" or "Agreement") concluded by Client with Unify Software and Solutions GmbH & Co.KG, Otto Hahn Ring 6, 81379 Munich, Germany, using "Click and Accept" when registering for the cloud service.

Client and Supplier shall individually be referred to as a "Party" and jointly referred to as the "Parties".

This DPA to the Agreement describes the Parties' obligations regarding the processing of Personal Data on behalf of Client, by Supplier, for the purposes of performing the Services set forth in the Agreement. Both parties shall act in accordance with applicable data protection principles, legal and contractual requirements.

1. Definitions

1.1. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Customer Agreement. Except as modified or supplemented below, the definitions of the Customer Agreement shall remain in full force and effect. For the purpose of interpreting this DPA, the following terms shall have the meanings set out below:

Term	Meaning
(a) "Applicable Laws"	means all current and future laws and regulations (as may be amended or updated from time to time) applicable to the Processing of Personal Data under the Agreement, including laws of the European Union or any Member State (which shall include, but not limited to GDPR), the United Kingdom, or any other applicable laws of any other country, province, state or jurisdiction to which the Processing of the Personal Data is subject.
(b) "Data Controller" (or Controller)	means the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the scope, purposes and means of the Processing of Personal Data.
(c) "Data Processor" (or Processor)	means a natural or legal person, public authority, agency, or any other body which Processes Personal Data on behalf of the Data Controller and as set forth in the written instructions of the Controller.
(d) "GDPR" or "General Data Protection Regulation"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 "on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC," as may be amended from time to time.
(e) "UK GDPR"	as defined in section 3 of the UK Data Protection Act 2018
(f) "Processing" (or any cognate terms)	means any operation or set of operations which is performed on Personal Data or on 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.
(g) "Personal Data"	means any information relating to an identified or identifiable natural person (a "Data Subject") pertaining to Unify (and the Data Subjects, respectively) Processed by Service Provider on behalf of Unify or an

Term	Meaning
	Unify Customer pursuant to or in connection with the Agreement. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as but not limited to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
(h) "Personal Data Breach"	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data which Unify Processes on behalf of Customer in connection with the Agreement.
(i) "Sub-Processor" or "Subcontractor"	means a third party engaged by a Data Processor which has or potentially will have access to or Process the Customer Personal Data.
(j) "Third Country"	means any country or jurisdiction outside of the country of origin or the European Economic Area ("EEA").

2. Roles and Obligations of the Parties

2.1 For the purpose of Processing Personal Data, both Parties acknowledge and recognize being bound by the duties and the obligations of the Applicable Laws and the following subsequent conditions.

2.2 The purpose of this DPA is to frame the Processing of Personal Data in connection with the terms of the Customer Agreement, regardless of the country of origin, place of Processing, location of Data Subjects, or any other factor.

2.3 The Parties expressly agree that (i) Customer is the Data Controller for the Personal Data Processed for the purpose of the provision of the Services under the Customer Agreement and (ii) Unify is the Data Processor in the event it Processes any Personal Data on behalf of and under the written instructions of Customer when performing the Services.

3. Guarantees regarding Customer's Processing

3.1. The Customer shall, as Data Controller, ensure that any Personal Data processed by Unify on its behalf is processed in accordance with the Applicable Laws and that it meets its own obligations in relation to the Processing of the Personal Data.

4. Exchange of Business Data and Communication Between the Parties

4.1 In the context of the performance of the Agreement, the Parties may be required, for the purpose of communication, to exchange the following information:

- personal information: first name, last name;
- communications data: telephone, email, postal mail; and/or
- other: Personal Data to which one Party provides access to the other for the purpose of communication between the Parties.

4.2 Both Parties undertake that each Party shall act as an independent Data Controller in order to process the above-mentioned Personal Data for their own means and purposes. Therefore, the Parties shall comply with the obligations of a Data Controller, as required by the Applicable Laws, in order to protect and secure the aforementioned Personal Data.

5. Customer's Processing Instructions

As a Data Controller, the Customer shall issue instructions to Unify as a prerequisite for Unify's processing of the Customer's Personal Data. These instructions shall initially be determined by the Agreement and may thereafter be amended, supplemented, or replaced by the Customer in writing or in an electronic format (text form) to the officer designated by Unify by means of individual instructions. Instructions which are not provisioned in the Agreement shall be treated as a change request. Verbal instructions shall be confirmed without delay in writing or in text form.

6. Unify's Obligations

6.1. Unify shall process Personal Data on behalf of Customer exclusively and only in accordance with the Instructions received from Customer as documented in Annex 1 to this DPA.

6.2. If Unify becomes aware that the instruction(s) it receives from Customer constitutes or may constitute an infringement of Applicable Laws, it shall immediately inform Customer in any written form of such actual or potential infringement.

6.3. Unify shall comply with any new lawful or revised Instructions provided by Customer. In case Customer's Instructions are or may be in contradiction with Applicable Laws, Unify shall stop Processing, or the part of the Processing that is infringing the Applicable Law and notify Customer as such in order to obtain new, revised and lawful Instructions.

6.4. Taking into account 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, Unify shall implement appropriate technical and organizational measures to ensure that Customer Personal Data are processed as per applicable legal data protection requirements as set forth in the Appendices of this DPA.

6.5. Unify confirms that its personnel in charge of processing Personal Data in the context of the Agreement are bound by an appropriate obligation of confidentiality regarding the Processing of Personal Data. Unify shall also ensure that its personnel in charge of Processing Personal Data in the context of the Agreement participate in mandatory training or e-learning regarding Privacy and Personal Data Protection.

7. Records of Processing Activities

Unify shall maintain a record of categories of Processing activities carried out on behalf of Customer regarding the Services provided under the Agreement, if required under Applicable Laws.

8. Data Subject Rights

8.1. Whilst Customer is responsible for determining the manner in which it responds to Data Subjects requests to exercise their rights under the Applicable Laws, Unify shall, in accordance with the Applicable Laws and taking into account the nature of the Processing, assist Customer by appropriate processes to support Customer in the fulfilment of the obligation to respond to Data Subjects' requests including notably:

8.1.1. promptly notify Customer if any Personal Data recipient receives a request that should have been directed to Customer from a Data Subject under any Applicable Law with respect to Personal Data;

8.1.2. ensure that the Personal Data recipient does not respond to that request, except on the documented instructions of Customer, where Customer and Unify have agreed that Unify shall undertake that role, or as required by the Applicable Laws to which the Personal Data recipient is subject, in which case Unify shall, to the extent permitted by

Applicable Laws, inform Customer of that legal requirement before the Personal Data recipient responds to the request; and

8.1.3. comply with any documented instructions from Customer regarding response to a request to exercise rights of the Data Subjects under Applicable Laws.

8.1.4. In this respect, parties shall communicate Personal Data in a structured, commonly used and machine-readable format.

9. Interactions with Supervisory Authorities

9.1. Upon Customer's request, Unify shall assist Customer with complying with its obligations towards any competent data protection authority where required, including:

9.1.1. providing information relating to a Processing where it is required to support a request for approval or authorization of a Processing;

9.1.2. providing information relating to a Processing in order to address any requests for information, controls or investigations; and/or

9.1.3. providing information in case of a Personal Data Breach as set out below in Section 15 of this DPA.

10. Security of Processing

10.1. Taking into account the state of the art, 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, Unify shall, in accordance with Applicable Laws, assist Customer to comply with its obligation to define and implement adequate technical and organizational measures to ensure the security and confidentiality of the Personal Data Processed under this DPA.

11. Data Protection Impact Assessments

At the request of the Customer, Unify shall provide the Customer with information which is required in order to enable the Customer to meet its legal obligations such as completion of a data protection impact assessment or providing an evidence of the technical and organizational measures taken to ensure data security.

12. Subcontracting

12.1 The Mitel Group owns and operates the Unify business. Unify is entitled to subcontract the Processing of Customer's Personal Data in whole or in part to other companies of the Mitel Group or to third parties for the purpose to comply with its obligations under the Agreement. Unify shall always inform the Data Controller of any intended changes with regard to the involvement or replacement of other Data Processors, giving the Data Controller the opportunity to object to such changes, which may not be refused without good cause under the Applicable Laws. If the Customer does not object within a period of 10 (ten) working days, the consent shall be deemed granted. If there is an important reason under Applicable Laws and if a mutually agreeable solution cannot be found between the Parties, the Customer shall be entitled to a special right of termination.

12.2 If Unify engages subcontractors for the Processing, it shall be obliged to transfer its data protection obligations under this Agreement to the subcontractor by means of corresponding agreements (contracts, binding internal data protection instructions, codes of conduct, etc.).

12.3 If such Processing includes a transfer of Customer Personal Data outside the EEA, the provisions set out in Section 13 below of this DPA shall apply.

12.4 The list of approved subcontractors of Unify in relation to the contractually agreed performance of Services is contained in Annex 1 to this DPA.

13. Transfers of Customer Personal Data to Third Countries

13.1. Unify and its affiliates are bound by the EU Standard Contractual Clauses as of June 4, 2021, according to GDPR Article 47.

13.2. Unify shall ensure that its third-party subcontractors authorized by Customer to Process Customer Personal Data provide an adequate level of protection for such Customer Personal Data. For that purpose, Unify shall: (i) ensure that any subcontractor authorized to Process Customer Personal Data outside the EEA shall comply with the obligations set out in appropriate standard contractual clauses for the transfer of Personal Data as set forth by the European Commission (or any competent authority) (in particular the European Commission's standard contractual clauses pursuant to Regulation (EU) 2016/679); or (ii) implement alternative means to the Standard Contractual Clauses in order to ensure an adequate level of protection of Customer Personal Data if acknowledged as appropriate by the competent European or local authorities.

14. Security and Confidentiality Measures

14.1. Customer acknowledges that: (i) the technical and organizational security measures defined and applied by Unify are based on the Instructions and information it has received from Customer, which are used to assess and evaluate, with Customer, the risks associated with the Processing of Customer Personal Data and (ii) it has reviewed the technical and organizational security measures set forth in Annex 2 (Information Security Requirements) and deems them adequate, taking into consideration the risks of the Processing, and the defined purpose of the Processing.

14.2. Customer agrees that, in the event that it modifies its Processing Instructions in accordance with the provisions of Section 5 of this DPA, the technical and organizational security measures initially defined and implemented may no longer be adequate to the risks of the Processing and the defined purposes of the Processing. In such case, Customer agrees that such technical and organizational security measures may need to be amended and that such changes may have an impact on the delivery of the Services and the terms of the Agreement, including, notably, the financial provisions.

14.3. Customer shall inform Unify in respect of any particular threats or vulnerabilities that it becomes aware of. Additionally, Customer acknowledges that significant security threats and vulnerabilities may, from time to time, occur and be identified by Unify. Where such threats and vulnerabilities result from or are connected to Customer's technical or operational decisions (e.g. initial security measures decided, systems implemented, etc.), Unify shall, without undue delay, notify Customer of said threat or vulnerability when it becomes aware of such threat or vulnerability. Unify shall, where possible, recommend a course of action or remediation to suppress, mitigate or limit the impact of the threat or vulnerability and the Parties shall agree to any such changes under the conditions set forth in Section 5 above. Customer shall bear any costs related to Unify's efforts to mitigate threats or vulnerabilities resulting from Customer's actions.

15. Personal Data Breaches

Unify shall notify the Customer without undue delay if it becomes aware of any Personal Data Breach concerning the Customer's Personal Data. Unify shall take the necessary measures to secure the Personal Data and to mitigate any possible adverse consequences for the data subjects and shall coordinate this with the Customer without undue delay.

16. Legal Requests for Access to Customer Personal Data

16.1. In the event Unify is requested or required under Applicable Laws or regulatory obligations to conduct certain Processing operations (including but not limited to disclosure to public authorities) relating to Customer Personal Data, in a Third-country that does not provide a level of protection to personal data that is essentially equivalent to that provided for in the EEA, and in the context of mass surveillance or surveillance measures Unify hereby expressly undertakes to: (i) inform Customer of such request or requirement as soon as possible (subject to compliance with legal provisions which may prevent it from informing Customer) in order to obtain Customer's express and written consent to such Processing operations; (ii) oppose, where possible, such request or requirement (including, notably, by advising that Unify does not own nor control the data it Processes on behalf of Customer); or (iii) assist Customer, if possible and at Customer's cost, in any action undertaken (if Customer so decides) to oppose such Processing operations.

17. Audit Rights

17.1. Customer may, once a year, and subject to prior written notice of at least four (4) weeks, conduct, or have an independent duly appointed third party established on the market for its auditing functions, an audit of Unify's Processing facilities in order to ensure Unify's compliance with the obligations set forth in this DPA. Any third-party conducting an audit on Customer's behalf shall be bound by a strict obligation of confidentiality and shall not be a Unify's competitor. Such audit shall not hinder or disrupt Unify's operations or business activities and shall only relate to that part of the relevant information technology infrastructure which processes Customer's Personal Data.

17.2. In addition to the annual audit right under 17.1 the Customer shall be entitled to perform additional audits in case of a Personal Data Breach; based on an order of a competent Data Protection Authority, or amendments in the applicable data protection legislation.

17.3 The party conducting the data protection audit shall bear its own audit costs.

18. No Selling of Personal Data

18.1. Unify acknowledges and confirms that it does not receive any Personal Data as consideration for any Services or other items that Unify provides to Customer. Customer retains all rights and interests in its Personal Data. Unify agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Unify to qualify as selling Personal Data under Applicable Laws.

ANNEX 1

GENERAL DESCRIPTION OF THE PROCESSING OF PERSONAL DATA CONDUCTED BY DATA PROCESSOR

Contact information

Unify affiliates	
Unify DPO	Name: _____ Post: gdpr@mitel.com Tel: _____

Service description

Please describe in few words the services or products provided by Unify to the Customer	Please, specify: Cloud Service Unify Phone 1 _____

Processing activities

Purpose of the Processing	Please describe the operation or set of operations which is performed on personal data Provision of the Cloud Services Unify Phone incl. Support. Further details for the use: *to be filled in by the Customer* • _____			
Categories of Processing activities* (see definition list below)	Collection*	☒	Consultation	☐
	Storage	☒	Media Handling (e.g. shipping of tapes or optical media)	☐
	Organization	☐	Disclosure	☐
	Structuring*	☒	Making available*	☒
	Recording	☐	Alignment/Combination/Matching	☐
	Adaptation	☐	Restriction of use or access*	☒
	Retrieval	☒	Erasure or destruction	☐
	Remote Access	☒	Use	☐
	Profiling	☐	(Big) Data-Analytics	☐
	Other (please, specify): *Collection – yes – Metadata *Structuring – not the main purpose *Making available – not the main purpose *Restriction of use or access – yes – by nature, but not the main purpose Disclosure – no - because it is not shared for the recipients own use Erasure or destruction - no - not beyond of legally required deletion of data • _____			
Location of the Data Subjects	European Union	☒		
	Non-European Union	☒		

	Please specify (non-EU): *As a cloud service provider located in the EU, Unify makes no assumption on the location of data subjects, since GDPR applies to all Data Subjects regardless of location. In case foreign data protection laws have to be fulfilled the customer is obligated to notify Unify for confirmation that such foreign laws are supported.*
Categories of Personal Data processed	Identification Data ☒ Connection Data ☒ Personal life ☐ Location Data ☐ Professional life ☒ Account profile ☒ Other (please specify):
Categories of sensitive Personal Data processed	No sensitive Personal Data ☒ Social Security Number or National Identification ☐ Trade-Union Affiliation ☐ Biometric Data ☐ Health Information ☐ Genetic Data ☐ Sexual Preferences ☐ Banking and financial data ☐ Criminal offences and sanctions ☐ Philosophical, Political or Religious Beliefs ☐ Telephone intercepts ☐ *The Cloud Service is not meant to process sensitive data, it is a Customer's decision whether to put such data as a content.*
Categories of Data Subjects	Employees of the Customer ☒ End-Users ☒ Customers of the Customer ☒ Members ☒ Suppliers ☒ Visitors ☒ Other (please, specify): *Data Subjects are users provisioned by the Customer for the Unify Phone Service and external callers leaving their phone number in logs and call journals. Unify makes no assumption about the affiliation of such data subjects with the Customer.*
Term of retention/deletion of Personal Data	Please, specify: Until termination of the contract. *Customer as a Data Controller may determine a different length during the customization process.*

Unify's Data Protection practices

Unify's guarantees regarding the Processing of Personal Data		Data protection/Privacy Policy/Binding Corporate Rules Reference : EU Standard Contractual Clauses as of June 4, 2021	☒
		Security standard certifications (e.g. ISO 27001) Unify is certified according to: • DIN EN ISO 9001: 2015 (Quality Management); • ISO / IEC 27001: 2013 (Information Security Management); • ISO / IEC 20000-1: 2011 (IT Service Management); • ISO / IEC 14001:2015 (Environmental Management) Reference: provide certification with link if requested by Customer	☒
		Regular training of employees on Data Protection	☒

Location of Unify Processing activities

Mitel Networks (Bulgaria) EOOD	2 Maria Luiza Blvd., TZUM Buisiness Center, 1000, Sofia, Bulgaria	Technical Support Services
Mitel Networks Romania S.R.L.	21st Mihail Kogalniceanu str. Bdg. C6/AP11, 500090 Brasov, Romania	Technical Support Services
Unify Communications Spain S.A.U.	25 Calle de Albarracin, 28307 Madrid, Spain	Technical Support Services
Mitel Networks Greece AE	455 Irakleiou Avenue, N. Irakleio, 14122 Athens, Greece	Technical Support Services
Unify - Soluções em Tecnologia da Informação Ltda.	Rua do Semeador, 702, Cidade Industrial - Curitiba City, Paraná State, Address Code (CEP 81.270-050), Brazil	Technical Support Services
Mitel Communications Private Limited	MIDC Plot B1 & B2 Software Technology Park 411062 Talwade, Pune, Maharashtra, India	Technical Support Services (Resource Pool)

Does Unify use one or several external subcontractors?

YES ☒

NO ☐

List of Unify's external subcontractors involved in the project

Google Ireland Limited	Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland	Data Center Services
MongoDB, Inc.	1633 Broadway 38th Floor New York, NY 10019, United States	Managed Data Base Service

The Cloud Service is hosted in data centers in the following countries:
Google Cloud Platform (GCP) region of Frankfurt a.M. (Europe-west3), Germany.

The MongoDB databases are installed in the Google Cloud Platform (GCP) region of Frankfurt (Europe-west3). Encryption at rest is used for the data encryption by Unify with keys owned and managed by Unify. MongoDB is a managed service. Unify creates the database on nodes installed and maintained by MongoDB.

Safeguards implemented if Unify's affiliates or subcontractors are located outside the EU or if Personal Data is available from outside the EU

Unify shall specify which measure it uses to frame the transfer of personal data to its subcontractors

Country recognized as providing an adequate level of protection by the EU Commission	☒
European Commission's Standard Contractual Clauses	☒
Specific (ad-hoc) data transfer agreement, requiring a high level of protection, duly validated by competent authorities	☐
Unify's validated binding internal data regulations	☒
Unify's adhesion to a validated code of conduct	☐

Please, specify:

_____

_____

* CATEGORIES OF PROCESSING ACTIVITIES	
Term	Definition
Adaptation	Providing services that transform existing data into a form more suitable for a particular purpose, for instance by removing data that is not required for that purpose or by making it accessible via a different means.
Alignment / Combination / Matching	Providing services that process two or more customer data sets in order to either (a) validate or update one or more of them, or (b) create a further data set.
Big Data Analytics	Providing the means for analyzing big data (big data is a massive amount of data sets that cannot be stored, processed, or analyzed using traditional tools). Big Data Analytics allows the accumulation and/or interrogation of large data sets for the purpose of deriving novel insights or new data sets. For example, a process used to extract meaningful insights, such as hidden patterns, unknown correlations, market trends, and customer preferences.
Collection	Providing services that can directly obtain data, such as: providing a website that receives applications, processing written data, or contacting individuals to obtain data.
Consultation	Providing services that require reference to existing customer data sets in order to answer queries on behalf of the customer.
Disclosure	Providing services that copy or transmit customer data to an authorized third party for its own use (for example a tax authority or a regulator).
Erasure or destruction	Providing services that permanently delete data so that it can never be recovered - either by securely wiping/overwriting it or by physically destroying the media that it is stored on.
Making available	Providing services that facilitate access to personal data, such as an internet or intranet service that provides user access to permitted data.
Media handling	Providing services that organize, store or transport media that contain customer's data.
Organization	Providing services improving data quality or accessibility, for example by bringing data together in one place or removing duplication.
Profiling of individuals	Providing services that analyze personal data from one or more sources leading to evaluation of certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. In other words, it identifies characteristics of identifiable individuals and/or make decisions, such as marketing decisions, that may subsequently have an impact on particular individuals (e.g. types of marketing they are sent or types of services they are offered).
Recording	Providing services that result in the storage of audio or video recordings., or creating data based on manual or automated observation to reproduce a scene. (e.g. electronic recording of voice or taking exact notes of a conversation)
Remote access	Providing the ability for an authorized person to access a computer or a network from a geographical distance through a network connection. It enables users to connect to the systems they need when they are physically far away.
Restriction of use or access	Providing services that allow specific data to be quarantined for example to meet legal obligations to restrict processing or to maintain evidential integrity of data for legal / regulatory purposes.
Retrieval	Providing services that process requests for finding personal data in, for example from archives or database. Retrieval is the operation of accessing data, either from memory or from a storage device.
Use	"Use" is non-specific and covers a multitude of other processing categories as listed here. Please only refer back to this term if the processing comprises all other categories except profiling, combination and Big Data Analytics. Data in use is data that is currently being updated, processed, erased, accessed or read by a system. This type of data is not being passively stored, but is instead actively moving through parts of an IT infrastructure
Storage	Providing services that offer the means for storing (i.e. kept for actual or possible further use) customer data, such as cloud storage, backup or archiving.
Structuring	Providing services that help to arrange data in a way that makes information more accessible and easier to use for its intended purpose.

ANNEX 2

INFORMATION SECURITY REQUIREMENTS

TECHNICAL AND ORGANIZATIONAL MEASURES

Technical and organizational measures (TOMs) are implemented according to the Technical and Organizational Measures Unify.

Notes:

1. These TOMs apply to the processing of personal data by Unify for the technical support of the Cloud Services resold under this Agreement.
2. Measures marked with N\A are out of scope for the technical support services delivered by Unify.
3. Measures marked with No*) are technically not possible for Cloud Services.

Confidentiality

Physical Access Control The goal of physical access control is to deny unauthorized persons access to those data Processing systems that process or use Personal Data.	**YES/NO**
Unify implements controls designed to stop unauthorized individuals to access to data Processing systems	YES
Unify uses a partitioning of Data Centre rooms	N/A
Unify uses a video surveillance and intrusion detection systems in order to monitor access to data Processing systems	N/A
Unify has policies ensuring physical access control	YES

Logical Access Control The goal of logical access control is to prevent unauthorized persons from using data Processing systems that process and use Personal Data.	**YES/NO**
Unify ensures that data Processing systems are accessed by means of authorization and authentication in all systems	YES
Unify assigns passwords to authorized persons	YES
Unify assigns a company ID to authorized persons	YES
Unify ensures that role-based rights are tied to access ID	YES
Unify uses encryption of data storage devices while in transit	YES
Unify ensures use of firewalls and antivirus software including regular security updates and patches	YES
Unify has policies ensuring logical access control	YES

Application Access Control Application access control measures prevent unauthorized Processing and activities (e.g. unauthorized reading, copying, modification or removal) in data Processing systems by persons without the required level of authorization.	**YES/NO**
Unify ensures the system-wide authentication of all users and data terminals including access regulations and user authorizations	YES
Unify implements a role-based authorization concept	YES
Unify ensures that access authorization is always based on the principle of restrictive allocation of rights	YES

Application Access Control Application access control measures prevent unauthorized Processing and activities (e.g. unauthorized reading, copying, modification or removal) in data Processing systems by persons without the required level of authorization.	YES/NO
Unify implements a program-related authorization concept	YES
Unify ensures that shared systems have client separation/separate data pool	YES
Unify has a clear desk policy in place	YES
Unify ensures that data storage devices in all mobile systems are encrypted while in transit	YES
Unify uses the firewalls and antivirus software including regular security updates and patches	YES
Unify carries out a regular review of all existing privileged accounts	YES

Separation Control The goal of separation control is to ensure that data collected for different purposes can be processed separately.	YES/NO
To the extent that there are no dedicated systems in use for exactly one customer, Unify ensures that the employed systems are multi-tenant capable	YES
Development and quality assurance systems are completely separate from productive systems in order to ensure productive operation	YES
Unify ensures that customer systems are only accessed by authorized persons from a secured administration network.	YES

Pseudonymization The objective of the pseudonymization regulation and control is that the Processing of Personal Data is carried out in such a way that the data can no longer be attributed to a specific Data Subject without additional information, provided that this additional information is kept separately and fall under the corresponding technical and organizational measures.	YES/NO
Unify uses anonymized identifiers, which can only be resolved using a separate database	NO
Unify uses server identifiers, which conceal conclusions on the function	NO
System hardening requirements include a strict prohibition on login banners with information about the type and version of the software used on the systems operated by Unify	NO

Encryption measures The aim of the measures for the encryption of Personal Data is to protect the contents of databases from unauthorized access and alteration.	YES/NO
Unify can ensure encryption of Personal Data following the given instruction from the controller	NO
Unify uses point-to-point or end-to-end SSL-encrypted data transfer between systems	YES
Unify ensures application-driven encryption of the data before transfer to databases	YES
Unify ensures encryption of DB backups	YES
Unify implements e-mail encryption	N/A

Schrems II Security measures for personal data subject to EU GDPR The aim of the measures for the encryption of Personal Data is to protect the contents of databases from unauthorized access and alteration in countries which do not ensure an adequate level of protection regarding mass surveillance laws and surveillance measures.	YES/NO
Unify ensures that the level of encryption and/or pseudonymization is adequate compared to the risk level in the country of importation as per the assessment conducted before the transfer.	YES
Unify ensures after encryption that the cryptographic keys remain either in the country of exportation, the European Union or in a third country recognized as providing a level of protection essentially equivalent to that guaranteed in the EU regarding mass surveillance laws and surveillance measures.	YES
Unify ensures in case of transfers of personal data to third countries mentioned above, the importer must not have access to the personal data unencrypted.	YES

Schrems II Security measures for personal data subject to EU GDPR The aim of the measures for the encryption of Personal Data is to protect the contents of databases from unauthorized access and alteration in countries which do not ensure an adequate level of protection regarding mass surveillance laws and surveillance measures.	YES/NO
Unify ensures that subject to request from Unify it will provide documented proof that cryptographic keys are located as per Unify' requirements.	YES

Integrity

Transmission control The goal of transmission control is to ensure that Personal Data cannot be read, copied, modified, altered or removed while being transmitted, transported or saved to a data storage medium and that it can be checked and asserted where the transmission of Personal Data through transmission systems is intended	YES/NO
Unify supports standard secure transmission types such as network-based encryption (server to server or server to client and/or to suppliers) and encrypted connection tunneling	YES
Unify uses SSL certificate for websites (https://) to transfer data within forms	YES
Unify has policy for mobile devices	YES
Unify implements disposal of data storage devices in a manner compatible with data protection regulations	N/A
Unify has clear desk policy in place	YES
Unify uses encryption of data storage media while in transit (including notebook hard drives)	YES

Input Control Measures that are suited for facilitating the belated checking and asserting if Personal Data has been entered into, changed within or deleted from data Processing systems and if so by whom	YES/NO
Unify has implemented access regulations and user authorizations that enable the identification of all users and data terminals in the system	YES
All monitoring and logging measures are adapted to the state of the art and the criticality of the data to be protected and carried out in the associated economic framework	YES

Availability and resilience

Availability control The goal of availability control is to ensure that Personal Data is protected from accidental destruction, damage or loss.	YES/NO
Unify ensures that Personal Data is stored at a minimum in systems which are protected against hardware-related data loss	YES
Unify ensures that Personal Data is stored in secure and redundant systems up to a spatially separate area, in order to ensure a short recovery time and a high overall availability	YES
Unify implements storage systems, in combination with appropriate software components, which are equipped with a technology that enables defined data from certain points of time to be recovered	YES
Unify carries out the data backups on a regular basis according to existing service agreements	YES
Unify ensures that the systems are powered without interruption	YES

Resilience / rapid recovery This measure ensures that Personal Data can be quickly recovered in the event of a physical or technical incident through an emergency management plan and regular recovery testing (at minimum annually	YES/NO
Unify ensures that emergency planning / crisis planning in connection with emergency and restart plans for the data centers is available	YES
Emergency plans are subject to a regular and continuous audit and improvement process	YES

Other measures

Privacy by Design and Privacy by Default	YES/NO
Unify ensures that Data Protection is taken into account at the earliest possible date by data protection-friendly presets in order to prevent unlawful Processing or the misuse of data.	YES
Unify minimizes the amount of Personal Data and ensures limitation of use	YES
Unify pseudonymizes or encrypts data as early as possible	YES
Unify creates transparency with regard to procedures and Processing of data	YES
Unify anonymizes data as early as possible	YES
Unify minimizes access to data	YES
Unify presets existing configuration options to the most privacy-friendly values	YES
Unify documents the assessment of the risks to the persons concerned.	YES