Data Processing Agreement (DPA) for Unify Cloud Services
For customers obtaining access to Unify Cloud Services via an Accredited Reseller

Version 2.1 as of July 2017

by and between

[Customer Name]
[Address]
[Address]
[Country]

hereinafter: “Controller” or “Customer”

and

[Accredited Reseller]
[Address]
[Address]
[Country]

hereinafter: “Processor”, or “Accredited Reseller”

Controller and Processor each a “Party” and, collectively, the “Parties”.

Scope

Unify Cloud Services are produced by Unify and provided to the Customer by the Accredited Reseller of Unify. Unify Cloud Services will allow the Customer and its Users to store information inside Unify Cloud. To the extent this information contains Personal Data, the Parties agree that this will be done by means of Commissioned Data Processing with Processor collecting, storing and processing such Personal Data only on behalf of the Customer as the Controller. The Processor for this DPA is the Accredited Reseller who in turn holds – now as the Controller – a DPA – directly or via a Distributor – with Unify as the ultimate processor of such Personal Data on Unify Cloud Services. This does however not rule out that also the Accredited Reseller processes Personal Data to some extent, which is also covered by this DPA. For the sake of clarity, this agreement on Commissioned Data Processing (hereinafter “DPA), is only applicable in jurisdictions where such DPA is required by mandatory law.

This DPA applies to the Personal Data collected through the Controller’s and the Controller’s Unify Cloud Services Users use of Unify Cloud Services. This DPA specifies the obligations of the Parties that arise between Controller and Processor from the Agreement. It applies to all activities carried out by the Processor within the framework of the Agreement whereby the Processor's employees or third parties commissioned by the Processor might handle personal data of the Controller.

The DPA does not apply to any other online or offline Unify products, sites, or services. With respect to Unify Cloud Services, this DPA prevails over any other existing data processing agreement or similar arrangement between Unify and the Customer that may already be in place for such other products, sites or services.

1. Definitions

In addition to the terms defined elsewhere in the Agreement, the following definitions apply:

1.1 "Personal Data" are individual elements of information concerning the personal or material circumstances of an identified or identifiable natural person.

1.2 "Commissioned Data Processing" means the storage, modification, transmission, blocking or deletion of Personal Data by the Processor acting on behalf of and following the Instructions of the Controller.

1.3 "Instruction" means a written order concerning a specific action with reference to Personal Data of relevance to data protection (for example, anonymization, blocking, deletion or making available) issued by the Processor. Instructions are specified in the Agreement and may be amended from time to time thereafter by the Controller if necessary, by means of separate, individual instructions. Instructions shall be given in writing and, where given orally, shall be confirmed by the Controller in writing (via letter or email) without undue delay.

2. Scope of Application and Responsibility; Relationship of this DPA to the Agreement

2.1 The Processor processes Personal Data only on behalf of the Controller.

2.2 The scope, type and purpose of the processing of Personal Data by the Processor are described in the Agreement and the Documentation, in particular the Product and Service Description (PSD).

2.3 The term of this Processing Agreement commences upon signature by both Parties or the commencement of the Agreement, whichever is earlier, and shall continue until the end of the term of the Agreement. Upon the expiry of the Agreement, this DPA shall terminate automatically together with the Agreement.

2.4 The following types or categories of Personal Data are generally collected, processed and used by the Processor:

- **Personal Data about the Unify Cloud Services Users you create**, in particular their user name, password, email address, access rights;
- **Personal Data derived from your Unify Cloud Services User's use of Unify Cloud Services**, in particular the IP-address used by the Unify Cloud Services User, the activity of the Unify Cloud Services User within Unify Cloud , the used bandwidth, storage space or CPU capacity, log-in/log-off times, all to the extent tht such data was not anonymized in order to generate aggregated Usage Data,
- **Personal Data that is present or placed by the Unify Cloud Services User in User Content**, such as Personal Data that is necessarily embedded in the content of the Conversations, e.g. in part of textual messages, documents, pictures, URLs and other User Content.

To the extent the Processor also collects, processes and uses Personal Data that is required for the conclusion and the performance of the Agreement, such as name, postal and email address, telephone number, name of the organizations and its address, separate billing address if any, IP-address, payment data, such Personal Data is out of the scope of this DPA.

2.5 The following parties are affected by the handling of their Personal Data within the framework of this agreement:

- Individuals working for the Controller as employees and including board members as well as shareholders to the extent they are individuals;
- Individuals working as freelancers for the Controller;
- Individuals working for external service providers of the Controller;
- Conversational partners of the above-mentioned persons, and
- Other participants to whom the Controller has granted the right to access his Unify Cloud Services Tenancy.

2.6 The Controller shall be solely responsible for compliance with the statutory data protection laws applicable to the products and services provided, or subscribed to, under the Agreement, especially for the legality of the transfer of Personal Data to the Processor and for the legality of the data processing. The Controller shall at all time be the "responsible body".

2.7 On the basis of this responsibility, the Controller may require the correction, deletion, blocking and making available of Personal Data both during the term of, and after the termination of, the Agreement.
Section 4.5 sentence 2 of this DPA shall remain unaffected thereby

Controller hereby confirms and acknowledges that in the event Controller requests Processor to delete or block his Personal Data, this may render the provision of the provided or subscribed-to products or services impossible. The Processor shall notify the Controller of such consequence before the execution of such Instructions.

2.8 This DPA shall also apply to the inspection or maintenance of automated processes or of data processing systems performed via remote access, if it cannot be excluded that access to Personal Data is possible when performing these tasks.

3. Duties of the Processor

3.1 The Processor may collect, process or use Personal Data only within the framework of this DPA and the Instructions given by the Controller. Material changes to the object of data processing and changes to the procedures must be agreed jointly and must be documented.

While Processor will not refuse any legally compliant Instruction by Controller, Controller acknowledges and accepts that some Instructions may result in additional remuneration claims for Processor. Processor will inform Controller accordingly prior to executing the Instruction. At any time and without limiting Processor's claim to additional fees, Controller may waive this right to be informed in prior, e.g. in urgent cases.

3.2 The Processor shall structure Processor's internal organization in a manner that is compliant with the specific requirements of the applicable Data Protection Regulations for the protection of Personal Data,. Processor shall take the appropriate technical and organizational measures to adequately protect Controller's Personal Data against misuse and loss in accordance with the applicable legal requirements in accordance with Applicable Data Protection Laws

3.3 The Processor shall provide the Controller with a summary of the technical and organizational measures , which is attached hereto as **Annex 1.** Controller understands that the technical and organizational measures are subject to technical progress and further development. In this respect, the Processor shall be permitted to use alternative, suitable measures.

3.4 Upon request, the Processor shall provide the Controller with information necessary for creating the processing description in accordance with Applicable Data Protection Laws.

3.5 The Processor shall provide that the personnel it uses for processing the Controller's data are bound by legal obligations to maintain data secrecy, and that they are informed about other applicable provisions concerning the protection of Personal Data, in particular telecommunications secrecy. The obligation to maintain data secrecy continues to apply after termination of their work contract.

3.6 The Processor shall provide the contact details of the Processor's data protection officer (DPO) on the internet. As of the effective date of this DPA, the DPO's current contact details can be found on the Controllers website.

3.7 The Processor shall inform the Controller in the case of breaches of regulations that protect the Controller's Personal Data or of if Controller's Instructions or Instructions from persons employed by the Controller were not properly observed.

3.8 The Processor shall be entitled to make backup copies of the Personal Data insofar as they are required to ensure correct data processing, and may copy and retain Personal Data that is needed for Controller's compliance with its statutory document retention obligations.

3.9 Processor shall store and handle media provided to Processor, and all copies or reproductions thereof, with care so that they are not accessible by third parties. The Processor shall be obliged to provide for a destruction of test material and other material containing Personal Data that is to be discarded on in a manner compliant with the law only on the basis of an individual commission by the Controller and at the latter's expense.

3.10 The fulfillment of the above-mentioned duties shall be controlled by the Processor and shall be evidenced in a suitable manner within the framework of the Controller's standard audit process as per section 6 hereof.

3.11 The Processor shall inform the Controller if the Processor is of the opinion that an Instruction is in breach of applicable statutory data protection laws and thereby fulfil its duty to notify under the applicable Data Protection Requirements. The Processor shall be entitled to suspend the implementation of the relevant Instruction until it has been confirmed or amended by the Controller.

4. Duties of the Controller

4.1 In respect of the Personal Data to be processed, the Controller and the Processor shall each be responsible for compliance with the data protection laws that are relevant to them. The Controller must inform the Processor if applicable laws, regulations or guidelines entail specific duties for handling Personal Data in a particular case.

4.2 The Controller shall inform the Processor promptly and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data that it becomes aware of.

4.3 Where it is legally required to keep and maintain a public directory of processing descriptions, this obligation rests with the Controller.

4.4 The Controller shall be subject to any data breach notification duties resulting from applicable Data Protection Requirements.

4.5 The Controller shall specify, contractually or by Instruction, the measures for the return of the media provided to Processor, and for the deletion of the Personal Data stored at the Processor after termination of this Processing Agreement.

The Controller cannot demand the deletion of Personal Data stored with the Processor insofar as the Processor is required by statutory law to retain material that contains that Personal Data, e.g. any applicable data retention rules.

Where Processor needs to retain Personal Data, it shall be blocked by the Processor until the applicable retention period has expired. In addition, Personal Data shall be blocked instead of deleting it, to the extent legally permitted under applicable Data Protection Requirements, in particular, if the deletion is not reasonably feasible or only possible with disproportional cost due to the particular type of storage.

4.6 Any additional costs incurred after this DPA was terminated due to the making available or deletion of Personal Data shall be borne by the Controller.

4.7 The Controller must notify the Processor in due time about changes in legal regulations in the area of data protection that affect the contractual duties of Processor and may require that this DPA be amended.

The Parties agree to bring about a mutually acceptable solution and to take into account the effects of this action on the agreed remuneration.

The Processor may also submit proposals to Controller if Processor deems a certain change to be necessary in order to remain compliant with Applicable Law.

5. Inquiries received by the Controller from Individuals

5.1 Where the Controller is obliged under Applicable Law to provide information to an individual about the collection, processing or use of its Personal Data, the Processor shall provide reasonable assistance to the Controller in making this information available, provided that:

- the Controller has requested the Processor in writing to do so, and
- the Controller reimburses the Processor for the costs incurred as a result of such assistance.

5.2 Insofar as an individual contacts the Processor directly for the purpose of correction of information about, or deletion of, its Personal Data, the Processor shall forward such request to the Controller who shall then instruct the Processor immediately as to how to proceed.

6. Audit Rights

6.1 With regard to the Controller's duty pursuant to applicable Data Protection Requirements to audit the Processor prior to the commencement of the data processing, and again during the term of the DPA, the Processor shall provide that the Controller may audit the technical and organizational measures undertaken by the Processor.

For this purpose, and upon explicit request of the Controller, the Processor shall furnish evidence to the Controller regarding the implementation of the technical and organizational measures pursuant to applicable Data Protection Requirements, by way of self-certification. Evidence for the implementation of such measures that do not relate exclusively to this specific DPA or the Agreement may also be furnished by submitting a current certificate, reports or extracts from reports by independent third parties, e.g. by certified public accountants, account auditors, the Processor’s internal and/or external data protection officer(s), the Processor’s IT security department, the Processor’s internal and external data protection auditors, quality auditors, or by a suitable certificate issued after Processor’s IT security or data protection were audited by a third party, e.g. in accordance with the German Federal Office for Information Security's (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) "*Grundschutz*" standard.

6.2 The Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit pursuant to section 6.1.

7. Subcontracting

7.1 The Controller agrees that the Processor may engage third parties for the provision of services contractually owned by the Processor.

7.2 If the Processor uses subcontractors who process the Controller's Personal Data, the Processor shall provide that such subcontractors are contractually obliged to comply with the applicable data protection laws. Upon written request of Controller, Processor shall inform Controller about the subcontractors engaged by Processor in connection with the Agreement who process Personal Data of the Controller as data processors of Processor.

7.3 In the event Personal Data may be transferred to, stored and processed in countries outside the EU, e.g. in the United States or any other country where Processor or Processor's Affiliates or subcontractors maintain facilities, Processor shall make the necessary contractual arrangements that are required under the EU Data Protection Regulations and the applicable local law (e.g. the German Federal Data Protection Act - Bundesdatenschutzgesetz, BDSG) for a legally compliant transfer, or processing, of Personal Data. If in order to achieve compliance with EU Data Protection Regulations it is required to enter into a direct contractual relationship between Controller and subcontractor, Processor shall coordinate with subcontractor and Controller to arrange for such direct contract to be closed, with this DPA serving as the benchmark.

8. Information Duties, Written Form Requirement

8. In the event Controller's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties, Processor shall inform Controller without undue delay, if permitted by law.

8.2 The Processor shall, without undue delay, notify all parties pertinent in such action that Personal Data affected by their measures is the Controller's sole property and at the Controller's sole disposition, and that the Controller is the responsible body pursuant to Applicable Law.

8.3 Any changes and additions to this agreement and to any of its elements, including any assurances by the Processor, shall require a written agreement and an express indication that it is a change or addition to these conditions. This shall also apply to any waiver of this written form requirement.

8.4 Intentionally left blank.

8.5 If any individual provision of the DPA is illegal, invalid, void, voidable or unenforceable, the remainder of the DPA will continue in full force and effect. The Parties shall agree upon an effective provision that, insofar as legally possible, most closely reflects what the Parties intended.

9. **Applicable Law, court venue**

9.1 If DPA executed in Germany
The contractual relationship shall be governed by the substantive law of Germany without regard to its principles of conflicts of laws. The court venue shall be Munich, save where another court venue is mandatory required Applicable Laws.

(City)	(Date)	(City)	(Date)
[Processor]		**[Controller]**	
Signature(s)		Signature(s)	
Name(s) in block capitals		Name(s) in block capitals	

Annex 1

General Technical and Organizational Measures pursuant to Section 9 BDSG and its Annex

effective 28 October 2014

Hereinafter, the material measures taken regarding compliance with the annex to section 9 BDSG, first sentence (control objectives No. 1 to 8), to the extent applicable, are briefly described.

The following description of the status quo of the elementary measures regarding the protection of data cannot cover any and all security measures in place. In particular in the context of data protection and data security, it is also not feasible to provide detailed descriptions of confidential measures, as the protection of security measures against unauthorised disclosure is as least as important as the security measure itself. In addition, the Service-specific Terms for Unify Cloud Services, in particular the Product & Service Description (PSD) and the Service Level Agreement (SLA), may contain further details about the technical and organizational measures undertaken.

The Customer is encouraged to discuss any individual questions relating to the technical and organizational measures with Customer's account manager at the Accredited Reseller.

1. Entrance Control ("Zutrittskontrolle)

Technical or organizational measures regarding access control, especially regarding legitimation of authorized persons:

The aim of the entrance control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Personal Data.

Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorizations. They are monitored by security personnel. Access for employees is only possible with an encoded ID with a photo on it. All other persons have access only after having registered before (e.g. at the main entrance).

Access to special security areas such as the service centre for remote maintenance is additionally protected by a separate access area. The constructional and substantive security standards comply with the security requirements for data centres.

2. System Access Control ("*Zugangskontrolle*")

Technical (password protection) and organizational (user master data) measures regarding the user ID and authentication:

The aim of the system access control is to prevent unauthorized use of data processing systems which are used for the processing and the use of Personal Data.

Each employee's user master data and individual identification code are registered in the global contact directory. Admission to the data processing systems is only possible after identification and authentication by using the identification code and the password for the particular system.

Additional technical protections are in place using firewalls and proxy servers.

In order to guarantee admission control, encryption technologies are used (e.g. remote access to the company network via VPN tunnel). The suitability of an encryption technology is measured against the protective purpose.

3. Data Access Control ("*Zugriffskontrolle*")

On-demand structure of the authorization concept and of the data access rights as well as their monitoring and recording:

Measures regarding data access control are to be targeted on the fact that only such data can be accessed for which an access authorization exists and that Personal Data cannot be read, copied, changed or deleted in an unauthorized manner during the processing, use and after the saving of such data.

Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorization concept. In accordance to the "need-to-know" principle, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.

In order to ensure data access control, an encryption technology is used (e.g. remote access to the company network via VPN tunnel). The suitability of an encryption technology is measured against the protective purpose.

4. Transmission Control ("*Weitergabekontrolle*")

Measures regarding the transport, transfer, transmission or storage of Personal Data on data media (manually or electronically) as well as regarding the subsequent review:

The aim of the transmission control is to ensure that Personal Data cannot be read, copied, changed or deleted without authorization during their transfer or while stored on data media, and that it can be monitored and determined to which recipients a transfer of Personal Data is intended.

The measures necessary to ensure data security during transport, transfer and transmission of Personal Data as well as any other company or customer data are detailed in the policy on the protection of confidential business information. In this policy, there is a detailed description of the entire processing of data, from the creation of such data to their deletion, including the handling of such data in accordance with their classification.

In order to ensure transfer control, an encryption technology is used (e.g. remote access to the company network via VPN tunnel). The suitability of an encryption technology is measured against the protective purpose.

The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service provider) is only made if a corresponding contract exists, and only for a specific purpose. If Personal Data are transferred to companies with their seat outside the EU/EEA, an adequate level of data protection exists at the target location or organization in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the EU model contract clauses.

5. Data Entry Control ("*Eingabekontrolle*")

Measures regarding the subsequent review, whether and by whom data were entered, altered or deleted:

The aim of the data entry control is to make sure with the help of appropriate measures that the circumstances of the data entry can be reviewed and monitored retroactively.

System inputs are recorded in the form of log files. By doing so, it is possible at a later stage to review whether and by whom Personal Data was entered, altered or deleted.

6. Data Processing Control ("*Auftragskontrolle*")

Measures (technical/organisational) to differentiate between the competences of principal and contractor:

The aim of the data processing control is to ensure that Personal Data which are processed by a commissioned data processor are processed in accordance with the Instructions of the principal.

Personal Data is used for internal purposes only (e.g. as part of the respective customer relationship). A transfer of Personal Data to a third party, such as a subcontractor, is only made under consideration of contractual arrangements and applicable data protection laws.

Details regarding data processing control are set forth in the corresponding Master Agreement and Processing Agreement.

7. Availability Control ("*Verfügbarkeitskontrolle*")

Measures regarding data backup (physical/logical):

The aim of the availability control is to ensure that Personal Data are protected against accidental destruction and loss.

If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.

Due to technical reasons, copies of Personal Data may be present in backup files and may be made by mirroring of services. Subject to processors' own statutory data retention obligation (see Processing Agreement), such copies are also deleted - if necessary, with a technically caused delay. The availability of the systems themselves is ensured in accordance with the necessary security level by corresponding security measures (e.g. mirroring of hard drives, RAID systems, USV).

8. Separation Control ("*Trennungsgebot*")

Measures regarding the separate processing (saving, changing, deletion, and transfer) of data with different purposes:

The aim of the separation control is to ensure that data which have been collected for different purposes can be processed separately.

Personal Data are used for internal purposes only (e.g. as part of the respective customer relationship). A transfer to a third party such as a subcontractor is solely made under consideration of contractual arrangements and data protection regulations.

Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability, the separation of functions as well as the separation of testing and production systems are used for this purpose.