



Unify Cloud Services

Information on Processing of Personal Data for Users

(Effective Feb 25, 2019)

If you are, or plan to become, a user of Unify Cloud Services, such as Circuit or OpenScape Cloud, this document is meant for you! Some of the data processed by Unify Cloud Services are your Personal Data (“Personal Data” means any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. (‘Data Subject’);

The processing of your Personal Data is protected by the **Applicable Data Protection Law, which** shall mean the laws and regulations relating to the processing and protection of Personal Data applicable in the country where Unify is established. In particular, Applicable Law means (a) EU Regulation 2016/679 (General Data Protection Regulation; ‘GDPR’) (b) Member State laws or regulations relating to the processing and protection of Personal Data implementing or complementing GDPR; and (c) any other applicable laws or regulations relating to the processing and protection of Personal Data.

Unify operates multiple Cloud services. You can identify whether you are a user of

- The EU instance by the URL <https://eu.yourcircuit.com>.
- The US instance by the URL <https://us.yourcircuit.com>.

How do we apply GDPR to Unify Cloud Services?

- First, Unify Cloud Services are meant for businesses, to allow employees, suppliers, partners and customers to communicate and collaborate with each other. As a result, not only you, but also the business which gives you access to Unify Cloud Services has rights with regard to the Personal Data processed by Unify Cloud Services.
- Secondly, Unify Cloud Services are delivered from one SW system via the Internet to 1000s of customers, or “Tenants” (meaning the legal entity you are an employee of and which has contracted for Unify Cloud Services), in exactly the same way. Tenants can set certain parameters or activate features in regards to data processing, but it is essentially the same for all tenants.
- Unify applies GDPR to both, the EU and the US instances of Unify Cloud Services

1 Controller – GDPR (articles 13.1a / 14.1a)

The Controller is directly accountable to you for the protection of your Personal Data. Among other responsibilities, the Controller, according to the GDPR,

- i. Defines the purpose of processing of your Personal Data
- ii. Defines the means of processing of your Personal Data

- iii. Responsible for Accuracy, Quality, Legality, Reliability of Personal Data
- iv. Provides information to you about your Personal Data and the modalities for the exercise of their rights
- v. Implements measures to secure and protect of your Personal Data
- vi. Notifies the competent data protection supervisory authority in case of a data breach.

For Cloud services like Unify Cloud Service, neither Unify nor your tenant can be the sole Controller. Instead we have a Joint Controller situation, as defined by the GDPR (article 26).

The responsibility split is as follows

- i. Your Tenant defines the purpose of processing of your Personal Data
- ii. Unify defines the means of processing of your Personal Data
- iii. Your Tenant is responsible for Accuracy, Quality, Legality, Reliability of Personal Data provided to Unify
- iv. Your Tenant provides information to you about your Personal Data
- v. Unify implements measures to secure and protect of your Personal Data
- vi. Your Tenant notifies the competent data protection supervisory authority in case of a data breach.

The GDPR requires Joint Controllers to sign a contract detailing the split of responsibilities. This document is called a Data Protection Agreement (DPA). You can find it under <https://unify.com/en/legal-information/dpa-for-unify-cloud-services>. You also have access to the DPA within Unify Cloud Service (Circuit / About) at any point in time.

The Unify entity identified as a joint Controller with Your Tenant is:

Unify Software and Solutions GmbH & Co. KG
Mies-van-der-Rohe-Strasse 6
80807 Munich, Germany,

hereunder “Unify” or “we”.

The second joint Controller is your Tenant. Your tenant is contractually obligated by the DPA to give you access to this document and to provide you will all the information that in its area of responsibilities it has to provide to you to comply with its obligations under the GDPR and which information we are not able to provide to you: for example the purpose of processing (i), i.e. what the Tenant wants to use Unify Cloud Services for.

2 Data Protection Officer – GDPR (articles 13.1b / 14.1b)

Unify has appointed a Data Protection Officer (“DPO”). You can reach the DPO at the following email address: dp.it-solutions@atos.net

Depending on the size of the business your Tenant might also have a Data Protection Officer. You have the right to get the contact details from your Tenant.

3 Purpose and Legal Basis for Processing – GDPR (articles 13.1c,d / 14.1c / 14.2b)

You have the right to understand the purpose and legal basis for the processing of your Personal Data in Unify Cloud Services. This is however the responsibility of your Tenant, as explained in section 1. Your Tenant has the obligation to provide You with this information. This will also determine which rights your Tenant claims in the data you enter into OpenScape Cloud Services, e.g. in form or work results of employees.

4 Categories of Personal Data – GDPR (articles 14.1d, 14.2(f))

Your Personal Data processed by Unify Cloud Services fall under the following categories:

- **Profile Data:** Personal data you create about yourself or are assigned to you by your tenant, in particular name, password, email address, photo, phone numbers, access rights (user vs tenant administrator).
- **Activity Data:** Personal data collected by Unify Cloud Services from your use of the services, in particular call journal data, content deletion or change records or data relating to service usage (e.g. used end-points). These data are collected to provide Call Journal functionalities and transparency to conversation members of Unify Cloud Services on who did what in a conversation, and for troubleshooting purposes. These data are also used in strictly anonymized form for usage, adoption, and user experience statistics and reports.
- **Transient and Session Data:** Personal Data which are collected but not stored on Unify Cloud Services (such as presence or location information) or which are tied to a log-on session on Unify Cloud Services (e.g. IP addresses). Location information is obtained from your browser or device if activated.

Notes:

- a) **Conversation Data**, i.e. postings, uploaded documents, and recordings you leave on Unify Cloud Services are generally not considered by Unify to be your personal data, but data for which your tenant has a certain degree of ownership. Please discuss possible concerns with your tenant
- b) **Private Address Books** may contain Personal Data of your personal contacts. Such Private Address Books are not stored and processed by Unify Cloud Services but reside in your phone. In general, all data you enter in your phone are controlled by yourself and are not subject to data protection by Unify Cloud Services
- c) **Statistics and Reporting Data** which Unify produces regularly from Activity Data and shares with tenants are strictly anonymized. You should be aware that tenants may ask for non-anonymized reports, which Unify may provide under certain circumstances. The usage of such reports and they compliance which GDPR, other laws, or applicable policies of business is entirely with the tenant. We recommend inquiring with your Tenant if such reports were requested from Unify or used, but you may also inquire with Unify.
- d) Please be aware that if you post information about a third person this might involve Personal Data of that person. Unify Cloud Services cannot recognize such information as Personal Data. We therefore have to exclude such data from our co-controller responsibilities. Please discuss such use cases with your tenant administrator or your DPO.
- e) A conversation with users from multiple tenancies belongs to the tenancy the user is from who created the conversation in the first place. You can find that user (“Creator”) under Conversation Details and view that user’s profile.
- f) If you join a conversation in a foreign tenant as a cross-tenancy user, your profile data will be shown in that foreign tenant, but remains stored in your home tenancy (the one that gives you access to Unify Cloud Services). Activity Data which are collected by your activities in the foreign tenant are stored in that foreign tenancy and are under the Co-Control of the foreign tenant.

5 Recipients of Personal Data – GDPR (articles 13.1e / 14.1e)

Data you enter into OpenScape Cloud Services including your Personal Data might be shared with third parties. You have the right to be informed about that:

Unify Cloud Services are all about communication and collaboration between its users. So it naturally shares information among users. Your Personal Data are disclosed to other users in your tenancy, and if you join upon invitation a conversation in a foreign tenancy as a cross-tenancy guest, your Personal Data will be disclosed to the members of that conversation unless you disable profile sharing with users of foreign tenancies (externals) under Circuit / Settings., Your Tenant Administrator can enable and disable that setting.

Your Profile Data will also be shared with your Tenant Administrators on Unify Cloud Services.

Unify will only share your Personal Data with approved internal or external sub-contractors for the purpose of delivering the service and supporting you as a user. Sub-contractors are listed in section 6.

Unify Cloud Services however have features which, when activated by the tenant administrator or by users, disclose Personal Data, for example

- Your Tenant might assign tenant administration privileges to the reseller the business purchased the cloud service from
- You might be invited to conversations in foreign tenancies of Unify Cloud Services as a cross-tenancy guest
- Unify Cloud Services might be federated with other cloud services or connected to your tenants VoIP system which will transmit some of your personal data. For more details see section 5.1 below on Cloud Service Integration

We only provide the technical features. You or Your tenant administrator activate these features and must be aware of which Personal Data will be disclosed and to whom and under which circumstances.

5.1 Out-of-the-Box Cloud Service Integration

For a number of popular cloud services, Unify offers an out-of-the-box integration with Circuit, which does not require any customization. This section describes how Personal Data are exchanged between Circuit and these cloud services:

Zapier

Cloud Service	Zapier	Flow of Personal Data
Provider	Zapier Inc.	Zapier is a workflow integration tool which allows connecting different apps to workflows. With the Circuit-Zapier integration, Circuit users can set-up Circuit as “trigger” for so-called “zaps”. In that mode, Circuit content (such as messages, message author names) can be pushed to third apps which are connected with Circuit in a work flow. Where the data is sent to is outside of Circuit’s control. With the Circuit-Zapier integration, users can also publish content from other cloud apps to Circuit. When this is done, Circuit only stores the content sent (and published to it). This content can be edited at any time within Circuit. No other data about the source of the content or credentials on external services is stored.
Account required	User Account	
URL	zapier.com	
Integration Authorization	by Tenant Administrator	
Integration Activation	by User	
Link to Data Protection Statements	https://zapier.com/privacy/	

Oauth based integrations such as Jenkins , Jira, Salesforce

Cloud Service	<ul style="list-style-type: none"> • Jenkins • Jira, • Salesforce,... 	Flow of Personal Data
Provider	<ul style="list-style-type: none"> • jenkins.io • Atlassian Corporation Llc • salesforce.com Inc. 	Oauth is an open standard for access delegation which allows cloud services like Circuit to obtain access to other cloud services. For all Oauth based integrations, the authentication is performed by the user on the third-party cloud service provider (Jira, Jenkins, ...) Circuit does not transmit nor stores the login / password of the user for that third party service. The only information Circuit holds is the access token for that user for that service. This token can be revoked by the user at any time, in his account management on the third party service platform. Information can then be pushed to Circuit from the other cloud platform, Circuit will store this information in the posted messages. These messages can be edited by the user at any time.
Account required	User Account	
URL	<ul style="list-style-type: none"> • jenkins.io • atlassian.com • salesforce.com 	
Integration Authorization	by Tenant Administrator	
Integration Activation	by User	
Link to Data Protection Statements	<ul style="list-style-type: none"> • jenkins.io/security/ • • 	

Cloud Storage Integration: Google Drive / Microsoft OneDrive / Box

Cloud Service	<ul style="list-style-type: none"> • Google Drive • Microsoft OneDrive • Box 	Flow of Personal Data
Provider	<ul style="list-style-type: none"> • Google Inc. • Microsoft Inc. • Box Inc. 	Circuit does not store any of your data on Google Drive. Conversely, Google Drive does not obtain Personal Data (see Section 4) from Circuit. When you authenticate on Google Drive from within Circuit, you authenticate directly against Google Drive. Circuit does

Account required	User Account	not process or store your login / password. Google Drive returns to Circuit an access token which is stored in Circuit alongside your user data. The Access Token can be revoked by you at any time (from the Google Drive account management). When you use the integration to browse your Google Drive, Circuit does not store nor caches the file list of your drive. When you share a file from your Google Drive using the integration, Circuit does not download, nor read or index the file. However, Circuit uses the Google API to make the file public and shares that link and the filename in the Circuit message. You may edit your message to remove the name and link to your file at any time.
URL	<ul style="list-style-type: none"> • drive.google.com • onedrive.live.com • www.box.com 	
Integration Authorization	by Tenant Administrator	
Integration Activation	by User	
Link to Data Protection Statements	<ul style="list-style-type: none"> • policies.google.com/privacy • privacy.microsoft.com/en-us/privacystatement • www.box.com/en-gb/legal/privacypolicy 	

6 Sub-Contractors and Transfers of Personal Data to Third Countries – GDPR (articles 13.1f / 14.1f)

Name	Address	Scope of Processing
IBM Deutschland GmbH	IBM-Allee 1, 71139 Ehningen, Germany	Data Center Services
Google Ireland Limited	Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland	Data Center Services
Atos IT Solutions and Services EOOD	Business park Sofia 1 / building 1B, Mladost IV, 1766 Sofia, Bulgaria	Technical Support Services
Atos IT Solutions and Services srl	Calea Floreasca nr.169A, Et. 2, Sector 1014459 București, Romania	Technical Support Services
Unify Communications S.A.	Paseo Doce Estrellas, 2. CP, 28042 Madrid, Spain	Technical Support Services
Unify Communications and Collaboration GmbH & Co. KG	Mies-van-der-Rohe-Strasse 6, 80807 München, Germany	Technical Support Services
Unify Enterprise Communications A.E	455 Irakliou Ave, Iraklio, 14122 Athens, Greece	Technical Support Services
Atos IT&Telecommunications Services SA	455 Irakliou Ave, Iraklio, 14122 Athens, Greece	Technical Support Services
Cycos AG Niederlassung Alsdorf	Joseph-von-Fraunhofer-Str. 7, 52477 Alsdorf, Germany	Technical Support Services
Atos IT Solutions and Services Inc.	1630 Corporate Court, 75038 Irving, TX, U.S.A	Technical Support Services
Unify Inc.	2650 N. Military Trail, Suites 100 and 250, 33431 Boca Raton, U.S.A	Technical Support Services
Unify - Soluções em Tecnologia da Informação Ltda	Rua Werner Siemens, 111, Prédio 20 05069-010 - Lapa – São Paulo – SP – Brazil	Technical Support Services
Atos India Private Limited	10th Floor, Tower-B, Hcc-247 Park, Lal Bahadur Shastri Marg, Vikhroli (W), Mumbai 400083 Maharashtra, India	Technical Support Services

Note that technical support services can be provided by Atos Group Companies located in India ,United States of America, or

Brazil to support different languages and time-zones. Unify belongs to the Atos group. Subcontractors within the Atos group (Unify, Cycos, Atos companies) are subject to Atos Binding Corporate Rules (see <https://atos.net/content/dam/global/documents/atos-binding-corporate-rules.pdf>) and EU Mandatory Clauses.

Storage Locations:

Storage Locations	Provider	Storage Locations	Provider
Circuit EU Instance (https://eu.yourcircuit.com)		OS Cloud EU Instance	
Amsterdam, Netherlands	IBM Deutschland	Amsterdam, Netherlands	IBM Deutschland
Frankfurt a. M., Germany	IBM Deutschland	Frankfurt a. M., Germany	IBM Deutschland
Circuit US Instance (https://us.yourcircuit.com)		OS Cloud US Instance	
Council Bluffs, Iowa, US	Google Ireland	Washington DC, US	IBM Deutschland
Berkeley County, South Carolina, US	Google Ireland	Dallas, TX, US	IBM Deutschland
		San Jose, CA, US	IBM Deutschland

Notes:

- a) Unify Cloud Services tenancies are provisioned *either* on the EU instance *or* the US instance You can verify the instance by the URL you use to access Unify Cloud Services
- b) Tenancies of EU tenants are generally provisioned on the EU instance, unless requested otherwise by the tenant
- c) Both instances are completely separated; there is no data flow between them.
- d) For the EU instance a local media and access node is deployed in the Sydney (Australia) data center contracted from IBM Deutschland, which gives access to users in the Asia-Pacific region and local conferencing capabilities. There is no persistent storage or personal data in this data center

Customer Notification: Migration to Google Cloud Services

Starting in the first quarter of 2019, we plan to begin the migration of the Unify Cloud Services from IBM data centers into the Google Cloud Platform in data centers in the following storage locations:

EU Instance (<https://eu.yourcircuit.com>):

- Frankfurt a.M. Germany
- Saint Ghislain, Belgium

US Instance (<https://us.yourcircuit.com>):

- Council Bluffs, Iowa, US
- Berkeley County, South Carolina, US

There will also be local media and access nodes in Googles data center in Sydney, Australia.

Customers who have signed up to Unify Cloud Services prior to November 21, 2018 have received a notification from Unify. Unify will update this document as the migration progresses to give an accurate status of the data centers used for data storage of Unify Cloud Services in the EU and US instance.

7 Data Retention – GDPR (articles 13.2a / 14.2a)

Retention of Personal Data, and the deletion of Personal Data, is managed in Unify Cloud Services on three levels

- 1) Retention managed by Unify
- 2) Retention managed by Tenant
- 3) Retention you can manage

7.1 Data Retention Managed by Unify

We don't delete data of Unify Cloud Services tenants on our own as long as the Cloud services agreement with the Tenant is in effect. Upon termination of the Unify Cloud Services agreement with your tenant, we delete all tenancy data at the end of the month following the effectiveness of the termination. As an example: if we receive a termination notice from the tenant or a reseller on April 14 with a notice period of three (3) months the termination goes into effect on July 15. At this point all access to the tenancy is suspended. We retain the tenancy with its data until end of August, in case the tenant wants to reverse cancellation or download data.

After this retention period after termination all tenancy data are deleted from the production system of Unify Cloud Services. They are still available in the automatic data-base back-ups we take to ensure high service availability. Back-ups still containing data of the terminated tenancy are finally deleted after 4 weeks. At this point tenancy data including your Personal Data are irreversibly deleted.

Profile, Activity, Transient and Session Data are included in client logs, which your Unify Cloud Services Client Software will collect if you use the "Report an Issue" feature on Unify Cloud Service Circuit. This data is transmitted to technical support centers of Unify Cloud Services listed in section 5 to allow support staff to conduct trouble shooting of the issue you reported. Such log data have a retention period of 6 months. Logging and tracing data which may be provided to software suppliers are anonymized.

Notes

- a) Termination notice period and retention after termination might be different for specific customer arrangements. Please inquire with your tenant if there are different arrangements agreed with Unify.
- b) Conversation and Activity Data you leave as a cross-tenancy guest in foreign tenancies are not affected by the termination of your Tenant (i.e. the one that gives you access to Circuit), but are still controlled by the foreign tenant. Please inquire with the foreign tenant on deletion.

7.2 Data Retention Managed by Tenant

Unify Cloud Services allow tenants to set a specific retention period (e.g. 24 months) for conversation data, i.e. postings, uploaded documents or recordings, counting from the day the data were entered by the user. Data which have aged beyond that retention period are automatically deleted with a 4 weeks delay for deletion in back-ups. This retention mechanism affects all users of the tenant.

If the Tenant removes you as a user of Unify Cloud Services, e.g. because you are leaving the company, the following will happen:

- Your Profile Data (see section 4) are deleted, except for your name
- Your Conversation Data (see section 4) are not deleted, nor are your Activity data, and they are still related to your name. We honor the right of Tenants in these data, since they might be important and valuable work results of your work for the business.
- For 4 weeks after deletion from the production data base deleted data will remain available in back-ups.

The tenant has however the following additional option (again with 4 weeks delay in back-ups):

- The tenant administrator can anonymize your name (or request anonymization from Unify) by a code name, while still retaining your Conversation Data, which are then not shown under your name any more but the code name.

The decision, which deletion method to apply, is with the Tenant. Please contact the tenant administrator or your DPO for questions.

Notes:

- a) Session Data are only stored as long as the session is active. Transient Data are not stored at all.
- b) Conversation and Activity Data you leave as a cross-tenancy guest in foreign tenancies are not affected by data retention managed by your home tenant (i.e. the one that gives you access to Circuit), but by the foreign tenant Please inquire with the foreign tenant on deletion

7.3 Data Retention You Can Manage

Unify Cloud Services give the following options to you as a user

- You can delete most of your Profile Data. If a data field cannot be deleted then it is because the data field was provisioned and is controlled by the tenant. Please inquire with your tenant about deletion.
- You can delete Conversation Data, but be advised that, if you do so, it creates an Activity log on the conversation that you deleted the post. This is because you shared your post with conversation members, and they should be able to know that you deleted the post.
- You can disable transient data, such as location and presence

What you cannot delete

- Your name from your conversation data, since this would affect other conversation members. However, unless provisioned by the Tenant, you make change your name for anonymization, if required.
- Activity Data, since this would also affect other conversation members and our ability to trouble shoot a technical problem which you might report to us
- Session Data during the session, since this would destroy the session.

8 Your Rights as a Data Subject and How to Exercise Them ()

Since your Tenant gives you access to Unify Cloud Services, and defines the purpose of its usage, we generally engage with the Tenant before executing a request. We therefore recommend that you place your request with the Tenant, who can give you an answer on your requests from the perspective of your business and execute most of your requests on the Tenant Administration for Unify Cloud Services. We have reserved the right from our tenants in the Data Processing Agreement that we may, after due consideration of the legal circumstances with the tenant, execute your request automatically, if required.

You can place requests in regards to your Personal Data with Unify either via the DPO shown in section 2 or via the following functional email address: askGDPR@atos.net

a) Right of Access to Personal Data – GDPR (article 15)

You can access all Personal Data directly on Unify Cloud Services. Your Profile Data are shown under Profile on Unify Cloud Services. For OpenScape Cloud (VoIP) your Circuit name is synchronized to the included with the VoIP back-end systems at Unify and with deployed phones. Your Activity Data are shown in the conversations you were active in, including the phone call conversation and depending on configuration also on phone devices. If you have been offline and e.g. missed calls this information will be shown on your Unify Cloud Services client.

b) Right to Rectification Personal Data – GDPR (article 16)

You can rectify most of all Profile Data yourself on Unify Cloud Services unless provisioned by your tenant, e.g. from a directory system of your business. Please contact your Tenant for rectification. If Activity, Transient or Session Data are incorrect, it is most likely because of a SW defect. Please use the mechanisms offered by your Tenant of Unify Cloud Services to open a trouble ticket.

c) Right for Erasure of Personal Data – GDPR (article 17)

Please see section 6 on Data Retention on details how to delete (erase) Personal Data. We recommend placing a request with your Tenant, but you can also place the request with Unify, in which case we would follow up with your tenant.

d) Right to Restrict Processing – GDPR (article 18)

Under specific circumstances, e.g. if you consider processing of your personal data inaccurate, unlawful, or no longer required, or if there is a pending objection from your side to the processing, you have the right to request a restriction of processing. We recommend placing a request with your Tenant, but you can also place the request with Unify, in which case we would follow up with your tenant. In case we restrict processing upon your request the following will happen:

- Your Profile Data will be deleted, and your name will be anonymized (service request)
- We keep your account in Unify Cloud Services including all conversation data accessible to conversation members, but not any longer under your name. Same with Activity Data
- You lose access to your account
- You can give your tenant or us instructions on further processing

If you decide to lift the restriction again and resume your account on Unify Cloud Services, your account will be unsuspended. You and your Tenant can re-enter your profile data, your conversation data will appear again under your name.

e) Right to Object Processing – GDPR (article 21)

You have the right to object processing of personal data under certain circumstances related to section 3 of this document (Purpose and Legal Basis for Processing). Since these establishing these criteria are with the tenant we recommend placing a request with your tenant, but you can also place the request with Unify, in which case we would follow up with your tenant.

f) Right to Withdraw Your Consent – GDPR (article 7.3 / 13.2c / 14.2d)

We do not collect consent from you in the sense of GDPR (6-7) as a legal basis for processing your Personal Data. Establishing that legal basis is the responsibility of your Tenant. In case your tenant collects your consent, you would have to withdraw that consent with your Tenant.

g) Right to Data Portability – GDPR (article 20)

You can cut and paste your profile data from Unify Cloud Services. There is no use of porting Activity Data. We do not allow users to download conversation data since we respect the rights your Tenant might have in your Conversation Data. Yet Unify Cloud Services give tenants the option to download the complete data stored in the tenancy or the data of a specific user only. We recommend placing a request with your Tenant, but you can also place the request with Unify, in which case we would follow up with your Tenant.

h) Right to lodge a complaint with a Data Protection Authority – GDPR (article 13.2d / 14.2d / 77)

You have the right to lodge a complaint about the processing described in this document with the data protection authority of your country or of the Federal Republic of Germany.

9 Is it a Statutory or Contractual Requirement to Provide Personal Data ? – GDPR (article 13.2(e))

Yes. As a user of Unify Cloud Services you must be identifiable to Unify and the tenant at least by your name and email address. Depending on the services you need to provide your business phone number. Beyond that Unify has no more requirements for you to provide your personal data, but your tenant might have. Please inquire with your Tenant in case of concerns.

10 Automated Decision Making

There is no automated individual decision making and profiling about you on Unify Cloud Services.