



Supplement to the list of processing activities pursuant to Art. 30 (1) GDPR for ProCall 6 Enterprise (SR1 / SR 2)

Contents

1	Foreword	2
2	Privacy-friendly default settings (Art. 25 GDPR).....	2
3	Reasons for GDPR proceedings (Art. 12 – 23 GDPR)	5
4	Rights of access, rectification or objection to processing	6
4.1	Rights of access (Art. 15(1) GDPR)	6
4.1.1	Purpose and legal basis of the collection, processing or use	6
4.1.2	Categories of personal data being processed	6
4.1.3	Rule deadlines for deleting the data or verification of the deletion	8
4.1.4	Origin of the data, where this has not been obtained by the data subject	8
4.2	Rectification (Art. 16 GDPR)	9
4.3	Objection	9
4.3.1	Erasure/ Pseudonymization (Art. 17 DSGVO).....	9
4.3.2	Restriction of processing (Art. 18(3) GDPR).....	10
5	Evidence of suitable technical and organizational measures according to Art. 24(1) and Art. 32 GDPR.....	13
5.1	Confidentiality (Art. 32(1) lit. b GDPR)	13
5.1.1	Protection against unauthorized access/access controls^	13
5.1.2	Access control (use of system).....	13
5.1.3	Access control (specific data)	14
5.1.4	Separation control	14
5.1.5	Pseudonymization	15
5.2	Integrity (Art. 32(1) lit. b GDPR)	15
5.2.1	Transfer control.....	15
5.2.2	Input control.....	15
5.3	Availability and resilience	16
5.3.1	Availability control	16
5.3.2	Recoverability	16

5.4	Procedure for regular verification, assessment, evaluation (Art. 32(1) (d) of the GDPR, Art. 25(1) GDPR)	16
5.4.1	Verification control	17
6	Hybrid cloud building blocks.....	17
	Additional information	17
	Legal information	17

1 Foreword

This document is intended to assist companies using ProCall software. The compiled information is intended to facilitate the preparation of a list of processing activities pursuant to Article 30(1) of the GDPR. It does not constitute legally binding information.

Such a list must contain all the details listed in Art. 30(1) sentence 2 lit. (a-g) GDPR. This information must give a meaningful description of the processing activities of the person responsible.

The preparation of records of processing activities does not in any way fulfill all the documentation requirements necessary by the GDPR. The list is only one building block in order to comply with the standardized accountability in Art. 5(2) GDPR. For example, the Conditions for consent (Art. 7(1) GDPR), the Responsibility of the controller (Art. 24(1) GDPR) and the result of Data protection impact assessments (Art. 35(7) GDPR) must be carried out so that the appropriate documentation can be verified.

The chapters are structured according to the procedural subject matter. Each chapter contains pre-filled information relevant to ProCall 6 Enterprise.

2 Privacy-friendly default settings (Art. 25 GDPR)

ProCall 6 Enterprise provides privacy-friendly default settings during the installation process. These can also be changed after the installation in the UCServer Administration:

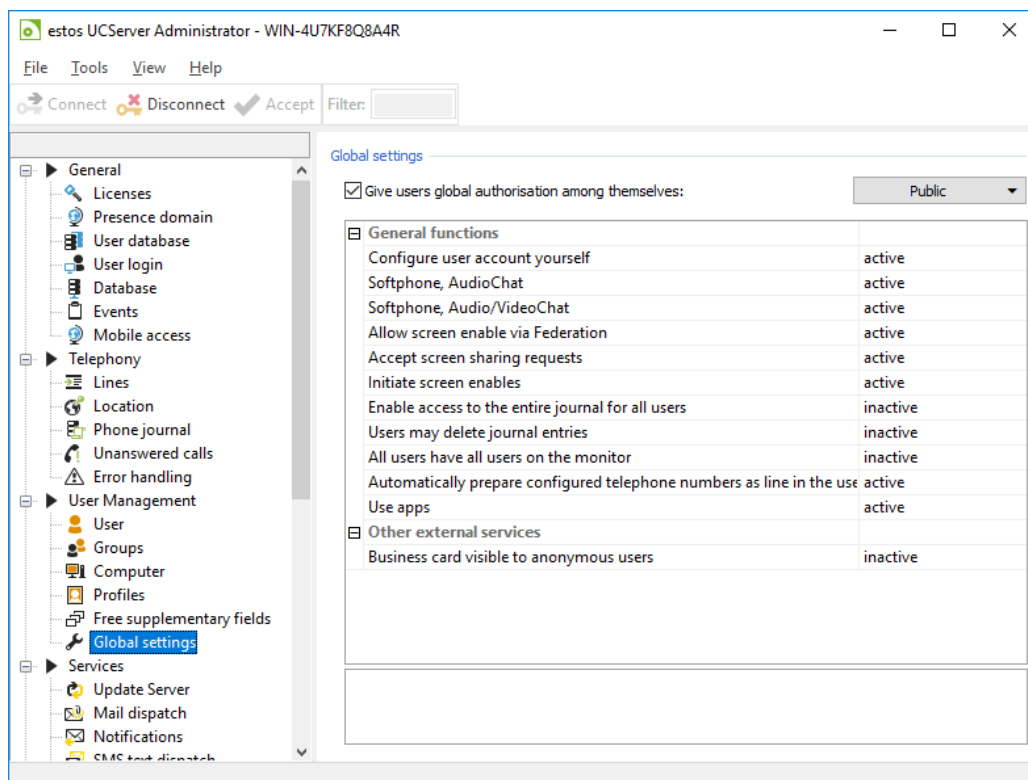


Figure 1. UCServer Administration with data protection-friendly basic settings

Further settings can be made via Profile Settings. These can be applied to users or entire user groups:

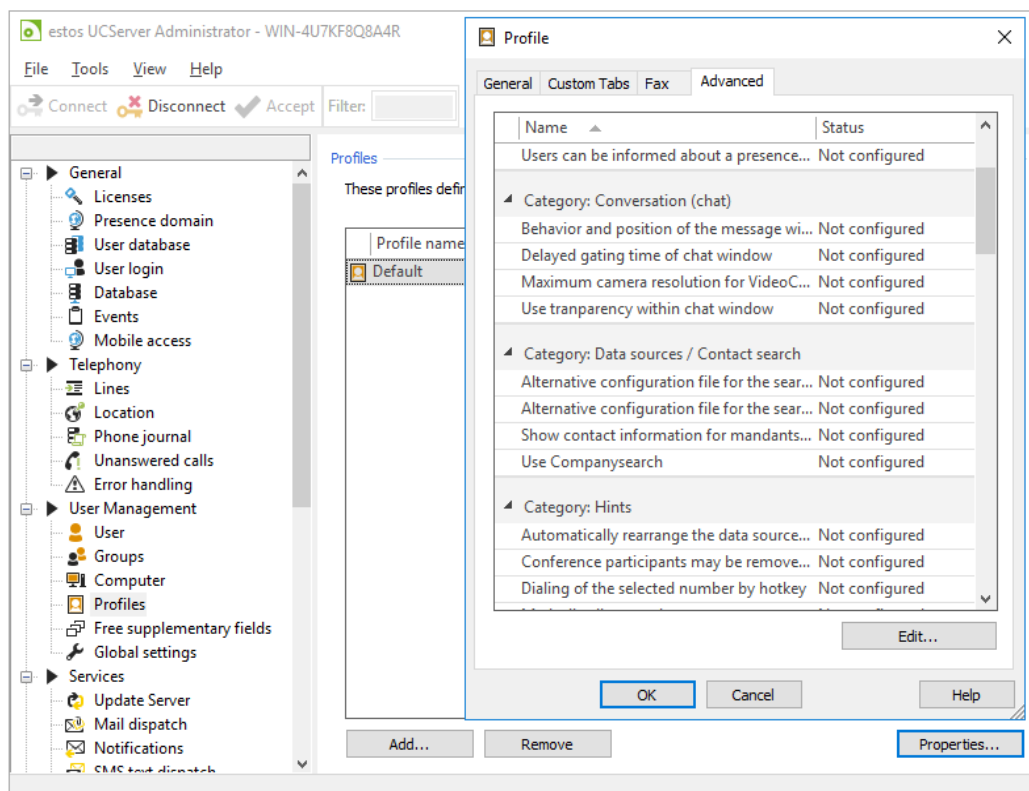


Figure 2. User profiles

Telephone journal entries are deleted automatically after a preset time:

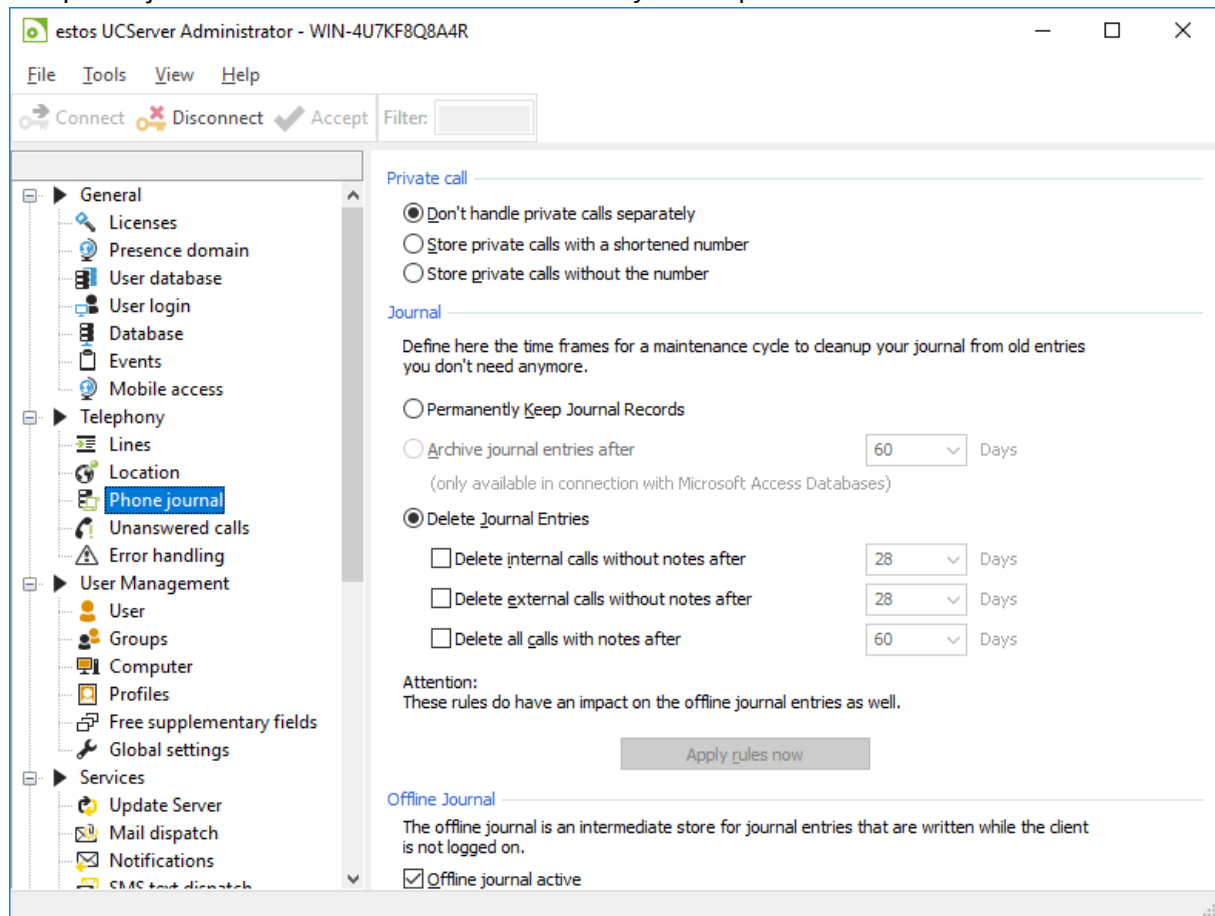


Figure 3. Automatic updating of the phone journal

The logging of (error) events can be limited:

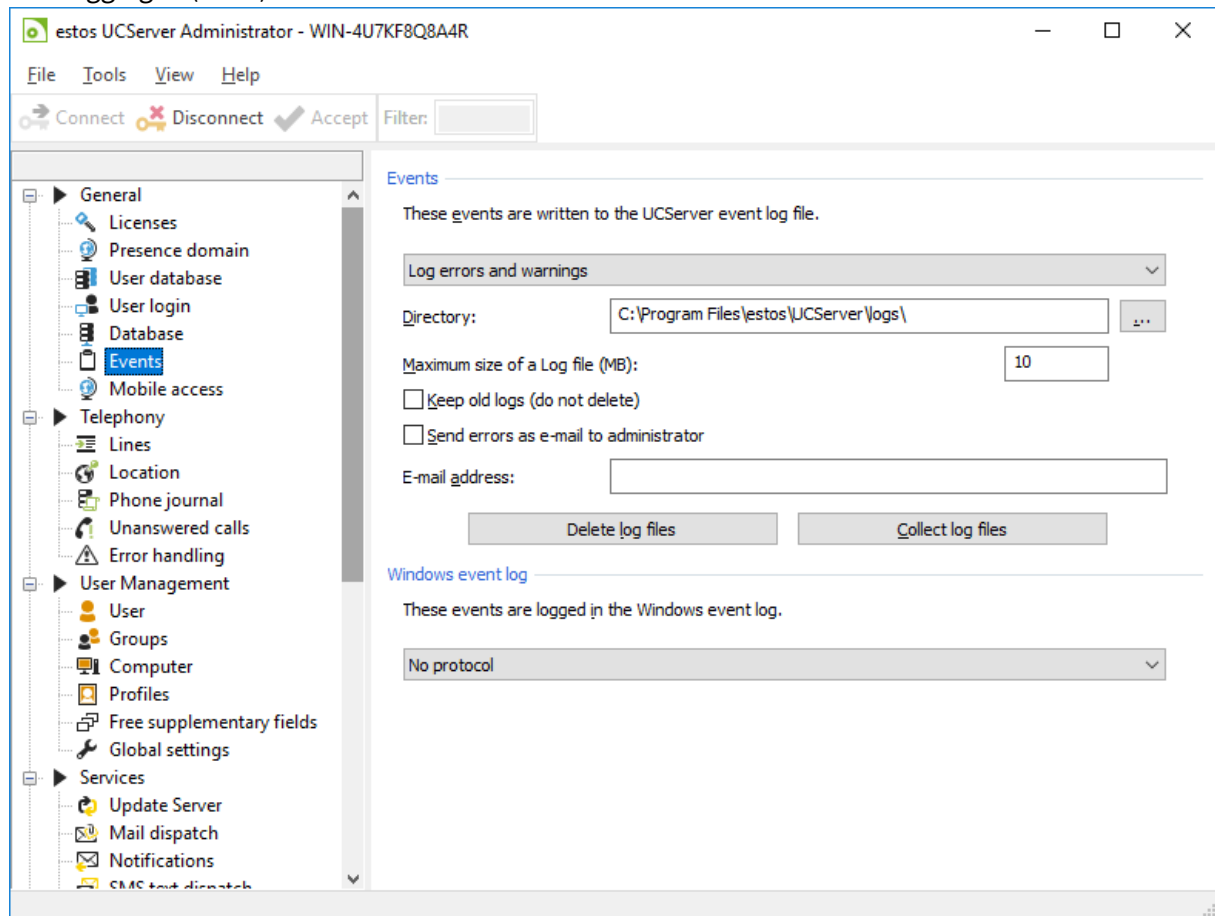


Figure 4. Limit error memory

3 Reasons for GDPR proceedings (Art. 12 – 23 GDPR)

Latest date of collected data sets (date of issue): _____

Is the reason due to rights of access, rectification or objection?

- **Right of access** (Art. 15(1) GDPR)
 - Right of access by the data subject (search criteria used): <Name>, <First name>, <Address street>, <Address postcode/town>, <Telephone number>, <E-mail address> etc.
- **Rectification** (Art. 16 GDPR)
 - Which person has requested rectification (search criteria used): <Name>, <First name>, <Address street>, <Address postcode/town>, <Telephone number>, <E-mail address> etc.
 - Which personal data must be changed: <Name>, <First name>, <Address street>, <Address postcode/town>, <Telephone number>, <E-mail address> etc.
- **Objection** (Art. 21 GDPR):
 - Erasure/pseudonymization (Art. 17 GDPR/Recital 26)
 - Restriction of the use of personal data (Art. 18(3) GDPR/Recital 67)

4 Rights of access, rectification or objection to processing

4.1 Rights of access (Art. 15(1) GDPR)

The information in this chapter provides information about the personal data processed in ProCall 6 Enterprise.

4.1.1 Purpose and legal basis of the collection, processing or use

Legal basis §§	Tasks for the fulfillment of which the personal data is collected, processed or used
Processor contract according to Art. 28 GDPR	Functions of the product: Favorites/Federation (F.x), Journal (H.x), Assignments/Tasks (T.x), Chat (C.x), Logs/Tracing (L.x)

4.1.2 Categories of personal data being processed

Group description such as health data, credit data, etc.

SEQ NO.	Name of the data (meaningful generic terms, e.g. names, addresses, details of technical fields in [] (square brackets))
F.x	Favorites/Federation:
F.0	User Principal Name (UPN)
F.1	Display name [displayName]
F.1.1	First name [givenName]
F.1.2	Surname [Sn]
F.2.1	E-mail address 1 [mail]
F.2.2	E-mail address 2 [mail2]
F.2.3	E-mail address 3 [mail3]
F.3	Job title/position [Title]
F.4	Company name [company]
F.5	Department [department]
F.6	Office/room number [physicalDeliveryOfficeName]
F.7	Public/private appointments
F.8.1	Subject
F.8.2	Time
F.9.x:	Address, business:
F.9.1	Street [streetAddress]
F.9.2	Postcode/ZIP [postalCode]
F.9.3	Town [L]
F.9.4	State/province [St]
F.9.5	Country [C]
F.10.x:	Address, private:
F.10.1	Street [privateAddressStreet]
F.10.2	Postcode/ZIP [privateAddressPostalCode]
F.10.3	Town [privateAddressCity]
F.10.4	State/province [privateAddressState]
F.10.5	Country [privateAddressCountry]
F.11.x:	Address, other:
F.11.1	Street [otherAddressStreet]
F.11.2	Postcode/ZIP [otherAddressPostalCode]

SEQ NO.	Name of the data (meaningful generic terms, e.g. names, addresses, details of technical fields in []) (square brackets)
F.11.3	Town [otherAddressCity]
F.11.4	State/province [otherAddressState]
F.11.5	Country [otherAddressCountry]
F.12	Note
F.13.1	Telephone, business [telephoneNumber]
F.13.2	Other telephone number [otherTelephone]
F.13.3.1	Mobile/cellphone number [mobile]
F.13.3.2	Mobile number, car [telephoneCar]
F.13.3.3	Mobile number, radio [telephoneRadio]
F.13.3.4	Mobile number, pager [pager]
F.13.4	Telephone, private 1 [homephone]
F.13.5	Telephone, private 2 [otherHomePhone]
F.13.6	Telephone, private (main number) [telephonePrimary]
F.13.7	Telephone number, company [telephoneNumberCompanyMain]
F.13.8	Telephone number, substitute [telephoneAssistant]
F.13.9	Telephone number, other
F.13.10	Telephone number, callback [telephoneCallback]
F.13.11	Telephone number, ISDN [telephoneISDN]
F.13.12	Telephone number, telex [telephoneTTYTDD]
F.13.13	Fax number, business [facsimileTelephoneNumber]
F.13.14	Fax number, other [otherFacsimileTelephoneNumber]
F.14	Photo [jpegPhoto]
F.15	Website URL [url]
F.16	SIP address (technical) [sipAddress]
F.17	Customer number [customerid]
F.18	URL for contact, e.g. in a CRM system [directWebLink]
F.19	Note [info]
H.x	Journal:
H.1	Display caller's name [PhoneNumber]
H.2	Caller's telephone number [LineNumber]
H.3	Display name of the called party (Spoken to)
H.4	Project name
H.5	Telephone number of the called party (MSN)
H.6	Date and time
H.7	Duration of the call
H.8	Extension of the called party (line)
H.9	Name of the called party's line (line name)
H.10	Display name of the original call partner during call forwarding (forwarded by)
H.11	Name of company
H.12	Caller's postal address (street, number, postcode, city, country, etc.)
T.x	Tasks:
T.1	Contact phone number [CallPhoneNumber]
T.2	Owner/responsible person [Owners]
T.3	Creator [Creator]
T.4	Completed by which person [CompletedFrom]
T.5	Contact name [DatabaseContact]
C.x	Chat:

SEQ NO.	Name of the data (meaningful generic terms, e.g. names, addresses, details of technical fields in [] (square brackets))
C.1.x:	SIP address (technical):
C.1.1	Participant
C.1.2	Sender
C.1.3	Recipient
L.x	Logging/Tracing:
L.1	Fields from F.x
L.2	Fields from H.x
L.3	Fields from T.x
L.4	Fields from C.x

4.1.3 Rule deadlines for deleting the data or verification of the deletion

Planned storage duration if possible, otherwise the criteria for determining the storage duration.

SEQ NO. from Chapter 3.1.2	Period
H.x	Adjustable from 1st day. Standard setting 90 days
F.x	Is assigned to the user of the contacts, that is, until the user is deleted from the system
T.x	Not possible
C.x	Not possible
L.x	Minimization of the amount of data by setting the data volume (size)

4.1.4 Origin of the data, where this has not been obtained by the data subject

The origin of personal data can be seen in the overview of contact details (Data source). The personal data/contact details can be accessed in the following areas (sequence no. from section 4.1.3):

- F.x: Favorites/Federation
- H.x: Journal
- T.x: Tasks
- C.x: Chat

4.2 Rectification (Art. 16 GDPR)

In ProCall 6 Enterprise, contact details are managed centrally and can therefore be changed centrally. Any changes to personal data are then effective throughout the software. Please refer to 4.1.2 Categories of personal data that are processed to find out which personal data can be changed in the software. You will find the corresponding correction option in the UCServer administration:

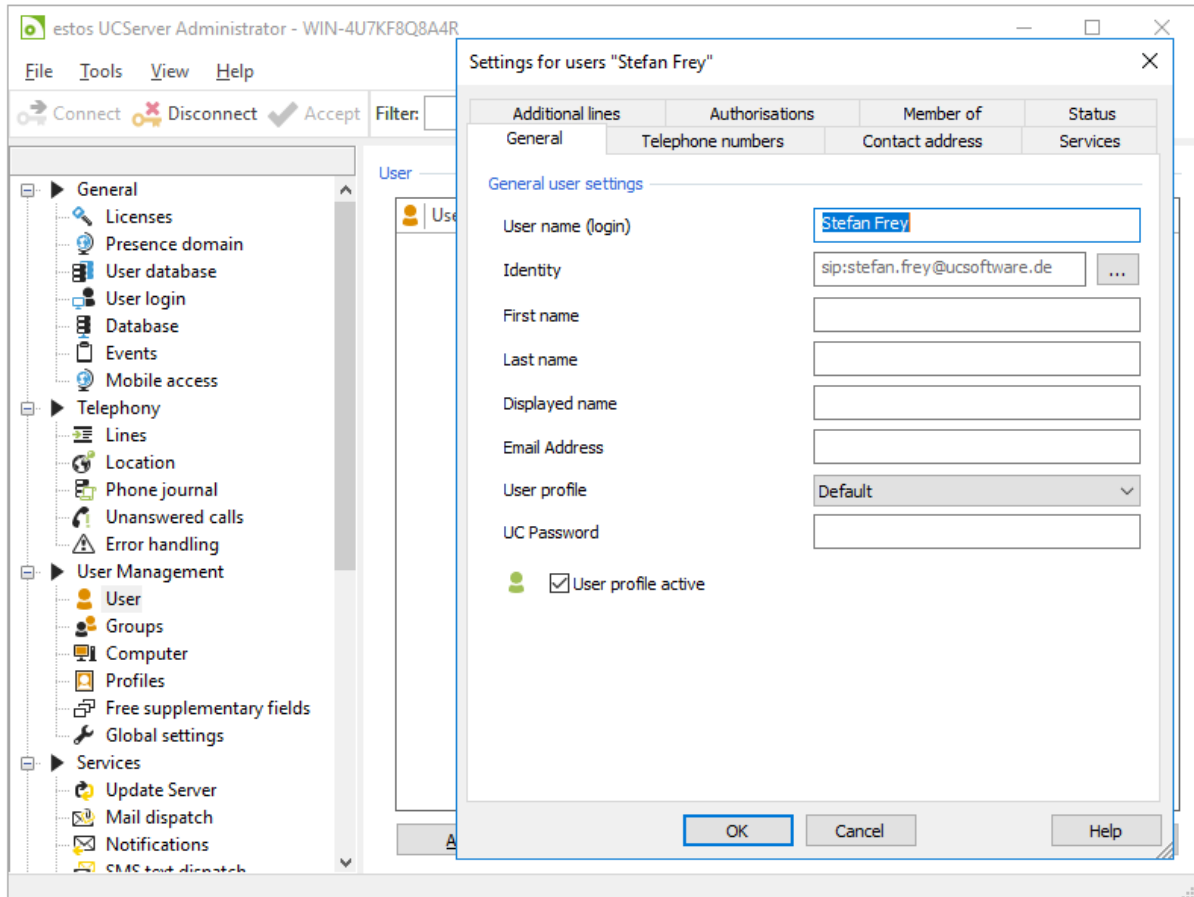


Figure 5. User administration and modification of personal data

4.3 Objection

4.3.1 Erasure/ Pseudonymization (Art. 17 DSGVO)

Pseudonymisation is currently not planned in ProCall Enterprise. Individual users or a selection of users can be deleted via the UCServer administration:

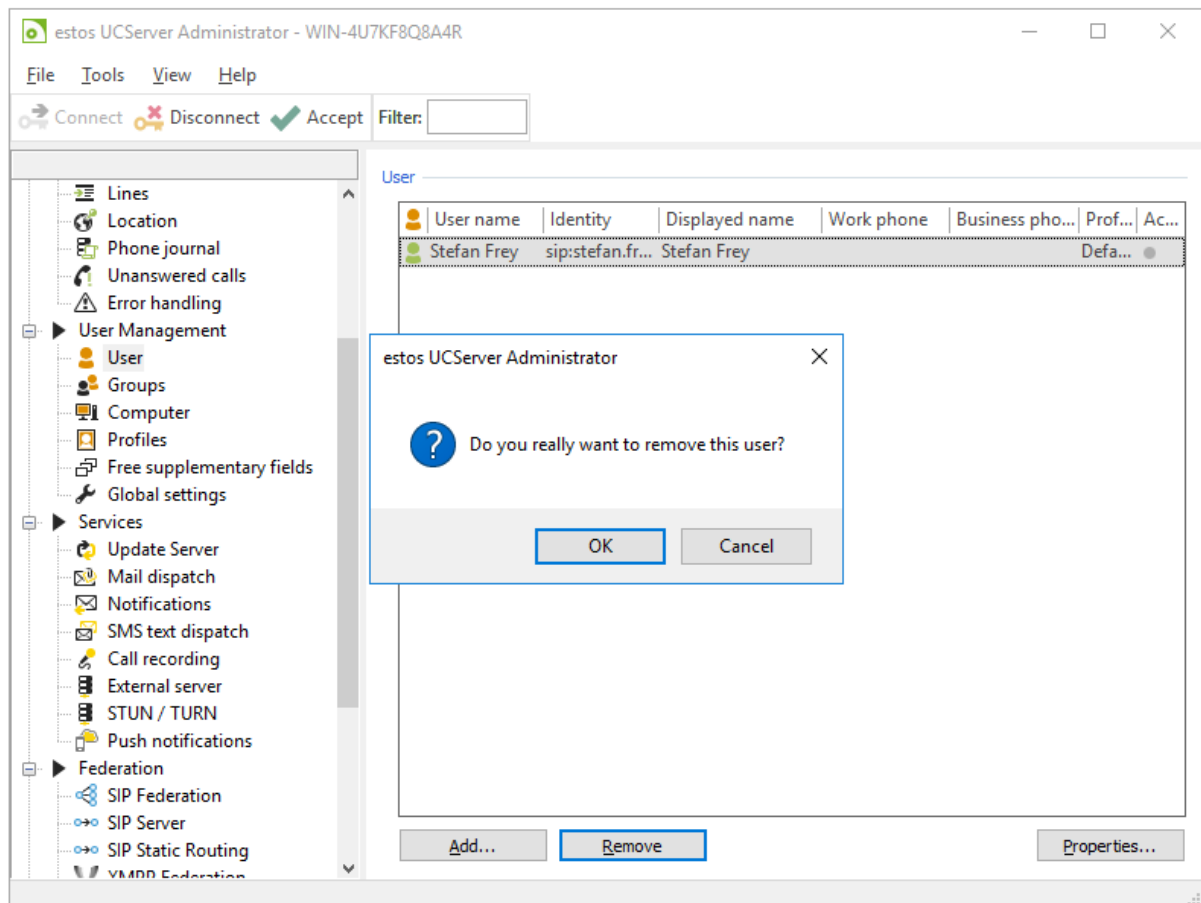


Figure 6. Deleting users in UCServer administration

4.3.2 Restriction of processing (Art. 18(3) GDPR)

ProCall Enterprise offers a number of ways to restrict the processing of personal data. These are described in detail below.

4.3.2.1 Journal

The data in the journal databases can only be viewed by the administrator. Administrator access is necessary for problem analysis and statistical evaluation.

The logging of data for private calls is carried out according to rules that can be configured.

The user can mark calls as private. Lines can generally be marked as private.

Selected telephone lines/extensions can be excluded from logging.

4.3.2.2 Presence states

Presence states or a change history of presence states are not logged. A possibility for the evaluation of presence states is not provided.

In the sense of an implementation of individual agreements, the exchange of presence-relevant information can be configured in a differentiated way.

The establishment of the lowest common denominator on the subject of presence within an organization can be done on three levels:

1. Global
2. Group
3. User

The rights system is additive, that is, if a right is assigned at a higher level, it cannot be removed at a lower level.

The presence state "Inactive" is displayed on a workstation PC or smartphone app due to "inactivity" and can be deactivated centrally/server-side. You can find the configuration in the UCServer administration in settings under User Administration Profiles.

4.3.2.3 Telephone function "Hands-free mode"

If the telephone system's CSTA interface provides the function "Switch to hands-free mode", this feature can be switched off via a compatible estos ECSTA middleware driver if necessary.


Telephone systems' "override functions" are generally not supported by estos ECSTA middleware drivers.

4.3.2.4 Authorization levels

Users themselves can control what selected (contact) details and actions a ProCall Enterprise user may view and perform via global authorization levels:

- **System-wide authorizations:**
If authorization is granted on a system-wide basis, it applies to all users of the system. These rights are assigned by the administrator.
- **Authorizations assigned to User Groups:**
If authorization is granted for groups, it applies to all users who are members of this group. These rights are assigned by the administrator.
- **Authorizations assigned by the user:**
Each user can assign individual authorizations to other users. These permissions can also be viewed and modified by the administrator.

The following authorization levels can be used to restrict the processing of personal data by ProCall Enterprise users as follows:

Overview of controllable (contact) details and actions for internal contacts/users					
Authorization level/(Contact) details and actions	Restricted 	Public	Business	Team member	Personal
Display name	Visible	Visible	Visible	Visible	Visible
E-mail address	Visible	Visible	Visible	Visible	Visible
Presence	Hidden	Visible	Visible	Visible	Visible
Chat	Prohibited	Possible	Possible	Possible	Possible
View public appointments	Hidden	Hidden	Visible	Visible	Visible
Extension 1: View outgoing phone numbers	Hidden	Hidden	Visible	Visible	Visible
Extension 1: View incoming phone numbers	Hidden	Hidden	Visible	Visible	Visible
Extension 1: View diversions	Hidden	Hidden	Visible	Visible	Visible
Extension 1: Call pick-up (Pick-up function)	Prohibited	Prohibited	Prohibited	Possible	Possible
Extension 2: View outgoing numbers	Hidden	Hidden	Hidden	Visible	Visible
Extension 2: View incoming numbers	Hidden	Hidden	Hidden	Visible	Visible
Extension 2: View call forwarding	Hidden	Hidden	Hidden	Visible	Visible
View private appointments	Hidden	Hidden	Hidden	Hidden	Visible
Extension 1: Set call forwarding	Prohibited	Prohibited	Prohibited	Prohibited	Possible
Extension 2: Set call forwarding	Prohibited	Prohibited	Prohibited	Prohibited	Possible
Extension 2: Call pick-up (Pick-up function)	Prohibited	Prohibited	Prohibited	Prohibited	Possible

Overview of controllable (contact) details and actions for external contacts in Favorites (Federation)					
Authorization level/(Contact) details and actions	Restricted 	Public	Business	Team member	Personal
Display name	Visible	Visible	Visible	Visible	Visible
E-mail Address	Visible	Visible	Visible	Visible	Visible
Presence	Hidden	Visible	Visible	Visible	Visible
Chat	Prohibited	Possible	Possible	Possible	Possible
Job title	Hidden	Visible	Visible	Visible	Visible
Name of company	Hidden	Visible	Visible	Visible	Visible
View public appointments	Hidden	Hidden	Visible	Visible	Visible
Telephone, business	Hidden	Hidden	Visible	Visible	Visible
Office	Hidden	Hidden	Visible	Visible	Visible
Address, business	Hidden	Hidden	Visible	Visible	Visible
SharePoint/website	Hidden	Hidden	Visible	Visible	Visible
Note	Hidden	Hidden	Hidden	Visible	Visible
Mobile/cellphone number	Hidden	Hidden	Hidden	Visible	Visible
View private appointments	Hidden	Hidden	Hidden	Hidden	Visible
Telephone, private	Hidden	Hidden	Hidden	Hidden	Visible
Other phone number	Hidden	Hidden	Hidden	Hidden	Visible

5 Evidence of suitable technical and organizational measures according to Art. 24(1) and Art. 32 GDPR

Here, the necessary measures for the creation and verification of suitable technical and organizational measures according to Art. 24(1) and Art. 32 GPDR for the software ProCall 6 Enterprise are described.

5.1 Confidentiality (Art. 32(1) lit. b GDPR)

5.1.1 Protection against unauthorized access/access controls^

How are the buildings in which the processing takes place secured against unauthorized access?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

How are the processing facilities protected against unauthorized access?

Access to personal data stored via an administrative password in the relevant system, for example, Microsoft Active Directory, LDAP directory service, or other data sources where personal information is stored.

The use of the UCServer administration is protected by the Microsoft Windows rights management and is additionally protected by an administrator password.

How are the implemented access control measures checked for suitability?

The software is subjected to regular in-depth testing.

5.1.2 Access control (use of system)

How to assign user access?

The administrator of the ProCall 6 Enterprise installation activates the users who can use the software.

It is possible to prevent the automatic setup of users.

How to check the validity of user accounts?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

How to document user access incl. application, approval procedure etc.?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

How do you ensure that the number of accesses by administration is reduced to only the necessary number and that only technically and suitable personnel are used for this purpose?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

Is access to the systems/applications from outside the company possible (home workstations, service providers, etc.) and how is access designed?

The use of ProCall Enterprise from outside the company is optional. The use of ProCall Mobile Smartphone Apps is ensured via hybrid cloud components (internet cloud) for which additional information is provided and is not the subject of this document.
See chapter 6 Hybrid cloud building blocks for more information.

5.1.3 Access control (specific data)

How do you ensure that passwords are only known to the respective user?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

What requirements are placed on the complexity of passwords?

Users login with their Microsoft Windows user login, or through individually configured username/password (integrated user administration).

How do you ensure that access authorizations are granted according to requirements and for a limited time?

Users who are authorized to use the software must be explicitly activated.

How do you ensure that the user can/must change his password regularly?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

What organizational precautions are taken to prevent unauthorized access to personal data in the workplace?

Access permissions are user and group-based for the people entrusted with the processing.

How does the documentation of access permissions occur?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

How do you ensure that access permissions are not misused?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

How long are logs kept?

See rule 4.1.3 deadlines for deleting the data or verification of the deletion.

Who has access to the logs and how often are they evaluated?

Only the system administrator has access to the logs.

5.1.4 Separation control

How do you ensure that data collected for different purposes is processed separately?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

5.1.5 Pseudonymization

What organizational measures have been taken to ensure that the processing of personal data complies with the law?

See 4: Rights of access, rectification or opposition to processing.

How is personal data processed/stored so that it cannot be assigned to the data subjects?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

5.2 Integrity (Art. 32(1) lit. b GDPR)

5.2.1 Transfer control

How is the integrity and confidentiality of the transfer of personal information ensured?

The data transmission is encrypted by technical means.

Are encryption systems used in the transfer of personal data and, if so, which ones?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

How is the disclosure of personal data documented?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

How is the unauthorized flow of personal data limited by technical measures?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

Is there a control system that can detect an unauthorized outflow of personal data?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

5.2.2 Input control

What measures are taken to understand who and when the applications were accessed and for how long?

There is a record (log) of logon and logoff information for all ProCall Enterprise clients and administration interfaces including a reference to the user.

4.1.3 gives time rules and the periods to apply to the deletion of the data or to the verification of the deletion.

How can it be seen which activities were carried out on the respective applications?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

What measures are taken so that the processing by employees can only take place in accordance with the instructions of the client?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

What measures are taken to ensure that the processing of personal client data by subcontractors is completed in the agreed scope?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

How is the deletion/blocking of personal data at the end of the retention period with subcontractors ensured?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

5.3 Availability and resilience

5.3.1 Availability control

How is the protection of data carriers against fundamental, external influences (fire, water, electromagnetic radiation, etc.) ensured?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

What protective measures are used to combat malicious programs and how is their timeliness guaranteed?

The ProCall Enterprise software is signed, which means any changes to the application would violate the signature and thus uncover any manipulation.

How do you ensure that any unnecessary or defective data carriers are properly disposed of?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

5.3.2 Recoverability

What organizational and technical measures are taken to ensure the availability of data and systems, even in the event of damage?

(Swift recoverability according to Art. 32(1) lit.c GDPR)

A backup function is included in the software. Possible applications for correction and objection (See 3: Reasons for GDPR proceedings) are not automatically accepted during a restore and must be checked and manually reworked since the last backup.

5.4 Procedure for regular verification, assessment, evaluation (Art. 32(1) (d) of the GDPR, Art. 25(1) GDPR)

What procedures are there for regular evaluation/verification to ensure the security of data processing (privacy management)?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

What will be the response to inquiries or problems (incident response management)?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

Which data protection-friendly default settings are there (Art. 25(2) GDPR)?

The base installation of ProCall Enterprise does not contain any personal information. Personal data can enter the product via the following means:

- Manual entry of contacts in
 - UCServer administration,
 - ProCall clients (desktop/smartphone)
- Connection of external contact data sources to UCServer and ProCall Client, e.g.
 - LDAP directory services (e.g. phonebook directory services, CRM/ERP systems, etc.)
 - Outlook contacts
 - Mobile phone contacts/phone journal synchronized via Bluetooth with ProCall desktop client
 - Microsoft Active Directory

5.4.1 Verification control

What are the processes for the directive or the handling of the order data processing (data protection management)?

By organizational measures that are not influenced or regulated by ProCall Enterprise.

6 Hybrid cloud building blocks

Further information on our hybrid cloud building blocks can be found on the internet at

<https://www.estos.de/anwendungen/cloud/ucconnect/> /
<https://www.estos.com/applications/cloud/ucconnect> .

Additional information

For further information about estos, e.g. about our products, services, data protection guidelines, code of conduct, can be found on our website. www.estos.de or www.estos.com

Legal information

The information in this document corresponds to our best knowledge at the time of publication. Errors and subsequent changes are reserved.

estos GmbH excludes any liability for damages that arise directly or indirectly from the use of this document.

Named brands and product names are trademarks or property of their respective owners.

Copyright estos GmbH. All rights reserved.

estos GmbH, Petersbrunner Str. 3a, 82319 Starnberg, Germany

info@estos.de

www.estos.de