Supplement to the list of processing activities pursuant to Art. 30(1) GDPR for ixi-UMS (from version 6.50)

Contents

1 Foreword

This document is intended to assist companies using ixi-UMS software (as of version 6.50). 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.

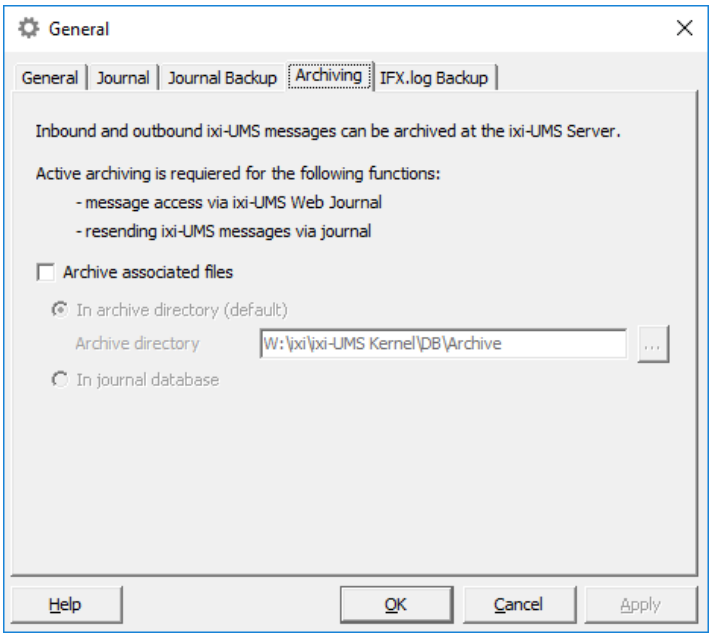
Such a list must contain all the details listed in Art. 30(1) sentence 2 lit. (a-g) GDPR. This information must give a meaningful description of the processing activities of the person responsible.

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.

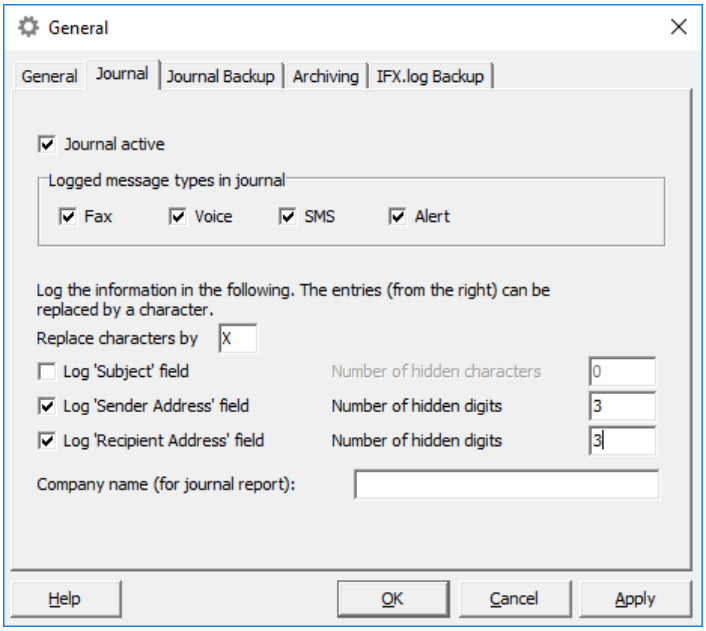
The chapters are structured according to the procedural subject matter. Each chapter contains pre-filled information relevant to ixi-UMS as of version 6.50.

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

ixi-UMS provides privacy-friendly default settings



ixi-UMS Enterprise offers additional privacy-friendly options



An extra tool provided allows the administrator to selectively delete and anonymize individual journal entries.

3 Reasons for GDPR proceedings

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

The information in this chapter provides information about the personal data processed in ixi-UMS (as of version 6.50).

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: Mail (M.x), Fax (F.x), Voicemail (V.x), SMS (S.x) Journal (J.x), User management (U.x), Logs/Tracing (L.x)

4.1.2 Categories of personal data being processed

(with group description such as health data, credit data, etc.).

Lfd. Nr.	**Name of the data (meaningful generic terms, e.g. names, addresses, details of technical fields in [] (square brackets)**
U.x	**ixi-UserManagement:**
	Title
	First name
	Surname
	Display name
	Description (any text)
	Street
	Mailbox
	Postcode/ZIP
	Town

	State/Province
	Country
	Company
	Department
	Department number
	Room number
	Employee number
	Phone numbers
	Fax numbers
	Mobile/cellphone numbers
	Pager number
	Private telephone numbers
	E-mail addresses
V.	Voicemail
	UMS number of the voicemail user
	Telephone number of the caller (when call number suppression is not activated)
	Voice message of the caller
F.	Fax
	UMS number of the fax user
	Fax number of the caller (when call number suppression is not activated)
	Content of the fax (i.e. the actual fax, as TIFF or PDF)
S.x	SMS
	UMS number of the SMS user
	Mobile (or landline) number of the SMS
	SMS message
M.1	Incoming UMS messages as e-mail
	Depending on the type of fax contents, SMS, voice (see above)
	The following data from MetaDirectory or similar, with the active sender identification feature
	Display name
	First name
	Surname
	Street
	Postcode/ZIP
	Town
	Company
	Sender's phone number
	Business phone number
	Mobile/cellphone number
	Fax number
	E-mail address
M.2	E-mail generated outgoing UMS message
	Depending on the type of contents of fax, SMS, voice (see above)
J.x	Journal

	Call number of the internal user, optional, any number of digits can be crossed out
	E-mail address of the user
	Call number of the external participant, any number of digits can be crossed out
	Subject of the message (for outgoing fax/voice/SMS messages), optional
L.x	Logs/Trace:
	Fields from M
	Fields from F
	Fields from V
	Fields from S
	Fields from J
	Fields from U

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.

Lfd. Nr. from Kap. 3.1.2	**Period**
M.x	None; Message is in user's mailbox, ixi-UMS has no access
F.x	Immediately after successful delivery (maximum attempts and duration are adjustable)
S.x	Immediately after successful delivery (maximum attempts and duration are adjustable)
V.x	Immediately after successful delivery (maximum attempts and duration are adjustable)
J.x	No duration adjustable; Administrator can delete "by hand"
U.x	No automatic deletion planned; Administrator can delete "by hand"
T.x	No automatic deletion planned; Administrator can delete "by hand"

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

a) Local user administration: entered by hand

b) User management in existing directory: from the configured data source (e.g. Microsoft Active Directory)

c) Contact data: from a single configured data source (e.g. MetaDirectory)

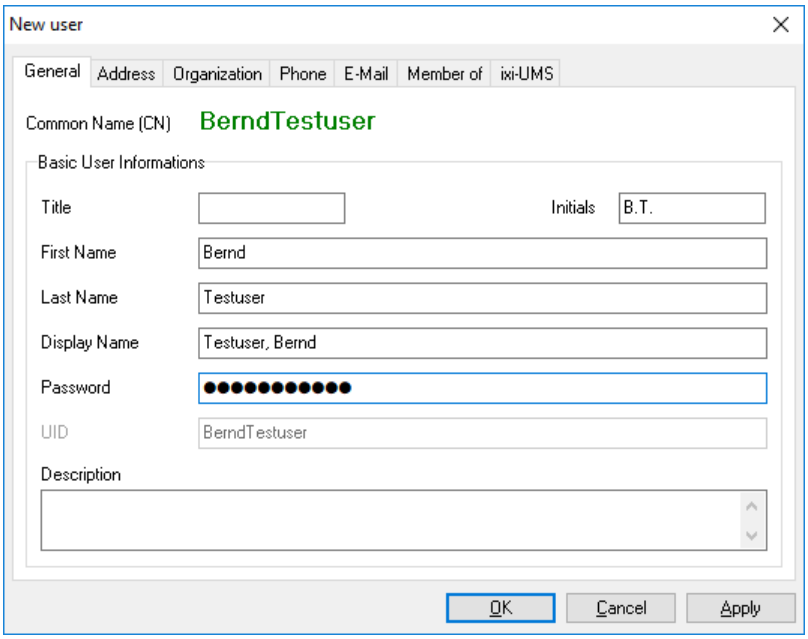
4.2 Rectification

Authorization takes place generally through the authorization concept of the operating and messaging/groupware system.

For local user management, ixi-UMS offers the following options

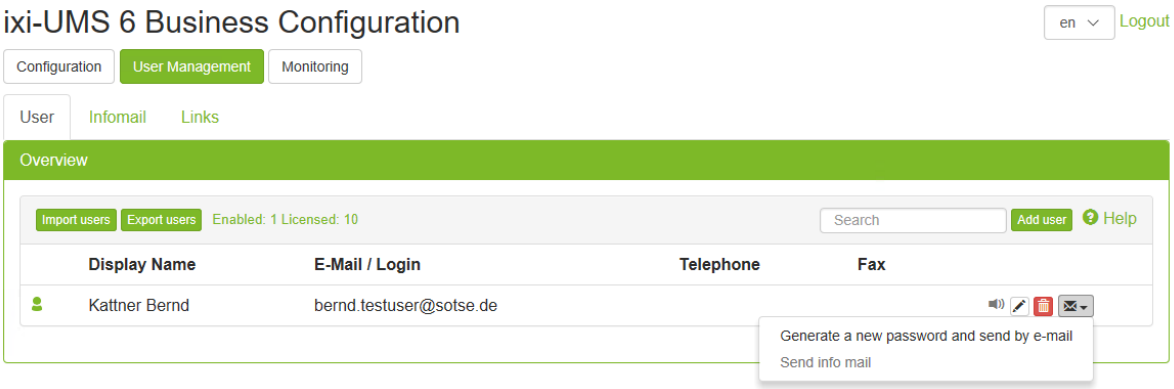
ixi-UMS Enterprise

In ixi-UMS Enterprise, it is possible for the administrator to assign a new password for the ixi-UMS-specific web applications.



ixi-UMS Business

In ixi-UMS Business, it is possible for the administrator as well as for users to assign a new password for ixi-UMS specific web applications.

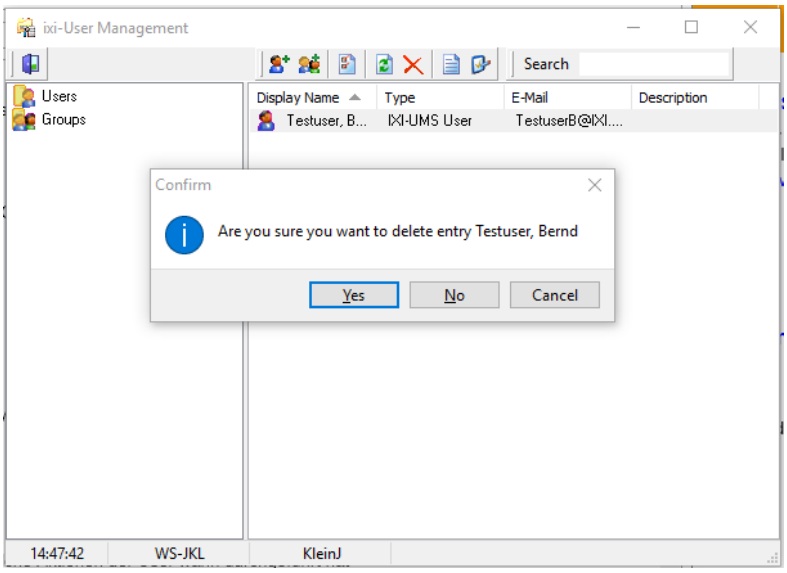


4.3 Objection

4.3.1 Anonymization (erasure)

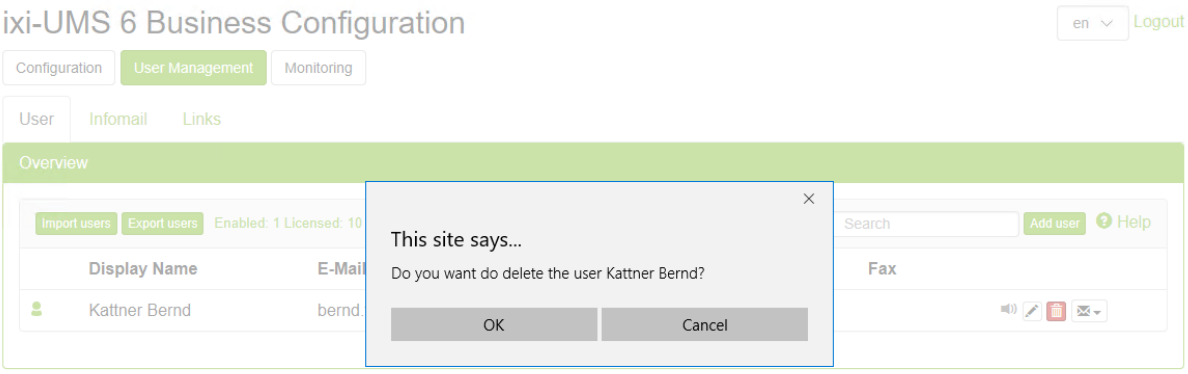
ixi-UMS Enterprise

Pseudonymization is currently not available in ixi-UMS Enterprise. Individual users can be deleted via the ixi-UMS Enterprise configuration.



ixi-UMS Business

Pseudonymization is currently not available in ixi-UMS Business. Individual users can be deleted via the ixi-UMS Business configuration.



4.3.2 Restriction of processing

ixi-UMS Enterprise offers a number of ways to restrict the processing of personal data. These possibilities will now be described in detail.

4.3.2.1 Journal

The data of all connections in the journal database can only be viewed by the administrator.

Sender identification, i.e. cancelling a contact based on the telephone/fax number, is optional.

Individual users' can only see the connections for their own account.

Internal user number, optional, any number of digits can be crossed out.

Call number of the external subscriber, any number of digits can be crossed out.

Saving the subject of the message (for outgoing fax/voice/SMS messages) is optional.

The journal can be switched off completely.

4.3.2.2 Trace/Log

Traces and logs can only be viewed by the administrator based on the authorization control of the operating system.

Trace/Log can be switched off completely (and is normally switched off in normal operation).

4.3.2.3 Mail

Sender identification, i.e. cancelling a contact on the basis of the telephone/fax number) is optional.

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 ixi-UMS from Version 6.50 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?
Organizational measure that is not influenced or regulated by ixi-UMS.

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 ixi-UMS administration is protected by the Microsoft Windows rights management (ixi-UMS Enterprise) or an administrator password (ixi-UMS Business). Exception: ixi-UMS Enterprise with local user administration.

How are the implemented access control measures checked for suitability?
As part of the QS tests that are performed on every release.

5.1.2 Access control (use of system)

How to assign user access?
By an administrator, depending on the type of installation in the existing user administration or in the ixi-UMS local user administration

How to check the validity of user accounts?
By organizational measures that are not influenced or regulated by ix-UMS.

How to document user access incl. application, approval procedure etc.?
By organizational measures that are not influenced or regulated by ix-UMS.

How to 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 ix-UMS.

Is access to the systems/applications from outside the company possible (home workstations, service providers, etc.) and how is access designed?
No; or only in the context of a VPN and similar methods that involve external users in the internal network.

5.1.3 Access control (specific data)

The initial password for ixi-UMS web applications is given by the administrator and can be changed by the user in the web application. For ixi-UMS Enterprise, this option can be turned on after installation.

What requirements are placed on the complexity of passwords?
Users login with their Microsoft Windows user login, or through individually configured username/password.

How do you ensure that access authorizations are granted according to requirements and for a limited time?
An authorized administrator can create, delete or change users as required in the directory (e.g. Active Directory or ixi-UMS user administration).

How to ensure that the user can/must change his password regularly?
If ixi-UMS is connected/integrated with Active Directory domain, the policies (Active Directory system settings) will allow you to change the password. If there is no connection to the Active Directory and the user management is integrated in the ixi-UMS instead, the user has the possibility to change the password in ixi-UMS via an ixi-UMS web application; With ixi-UMS Enterprise this possibility can be switched on and off.

What organizational precautions are taken to prevent unauthorized access to personal data in the workplace?
By organizational measures that are not influenced or regulated by ix-UMS.

How does the documentation of access permissions occur?
By organizational measures that are not influenced or regulated by ix-UMS.

How do you ensure that access permissions are not misused?
By organizational measures that are not influenced or regulated by ix-UMS.

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; partly secured by ixi-UMS itself and partly secured by authorization from the operating system.

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 ix-UMS.

5.1.5 Pseudonymization

What organizational measures have been taken to ensure that the processing of personal data complies with the law?
By organizational measures that are not influenced or regulated by ix-UMS.

How is personal data processed/stored so that it cannot be assigned to the data subjects?
With the exception of the journal, no personal data is kept/stored; possible anonymization possibilities in the journal are shown crossed out in 4.1.2.

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

5.2.1 Transfer control

How to ensure the integrity and confidentiality of the transfer of personal information?
By organizational measures that are not influenced or regulated by ix-UMS.

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 ix-UMS.

How is the disclosure of personal data documented?
By organizational measures that are not influenced or regulated by ix-UMS.

How is the unauthorized outflow of personal data limited by technical measures?
By organizational measures that are not influenced or regulated by ix-UMS.

Is there a control system that can detect an unauthorized outflow of personal data?
By organizational measures that are not influenced or regulated by ix-UMS.

5.2.2 Input control

What measures are taken to understand who and when the applications were accessed and for how long?
For ixi-UMS web applications, ixi-UMS can record the log-on and log-off attempts as well as any actions performed by all users.

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 ix-UMS.

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 ix-UMS.

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 ix-UMS.

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 ix-UMS.

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 ix-UMS.

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

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

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

By organizational measures that are not influenced or regulated by ix-UMS.

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)

ixi-UMS can be implemented in cluster operation and are completely redundant. For example, storing the few persistent files: the journal can be a RAID/NAS system.

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 ix-UMS.

What will be the response to inquiries or problems (incident response management)?
By organizational measures that are not influenced or regulated by ix-UMS.

Which data protection-friendly default settings are there [Art. 25(2) GDPR]?
The base installation of ixi-UMS does not contain any personal information. Personal data can enter the product via the following means: • local user administration; default setting is usage of existing user management such as: e.g. Active Directory For fax/SMS/voice mailing, journal data is created; The journal can be switched off completely, telephone numbers can be partially or completely crossed out.

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 ix-UMS.

6 Additional information

For further information about estos, our products, services, privacy policy, and code of conduct, please visit our website www.estos.de or www.estos.com

7 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.

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

info@estos.de

www.estos.de