



Ergänzung zum Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO für ixi-UMS (ab Version 6.50)

Inhaltsverzeichnis

1	Vorwort	2
2	Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO).....	3
3	Anlässe für ein DSGVO-Verfahren.....	4
4	Rechte auf Auskunft, Berichtigung oder Widerspruch der Verarbeitung.....	4
4.1	Auskunft	4
4.1.1	Zweck und Rechtsgrundlagen der Erhebung, Verarbeitung oder Nutzung	4
4.1.2	Kategorien personenbezogener Daten, die verarbeitet werden	4
4.1.3	Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung.....	6
4.1.4	Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden	6
4.2	Berichtigung.....	7
4.3	Widerspruch.....	8
4.3.1	Anonymisierung (Löschung)	8
4.3.2	Einschränkung der Verarbeitung	8
5	Nachweis geeigneter technischer und organisatorischer Maßnahmen nach Art. 24 Abs. 1 und Art. 32 DS-GVO	9
5.1	Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO).....	9
5.1.1	Schutz vor unbefugtem Zugang / Zugriffskontrollen	9
5.1.2	Zugangskontrolle	10
5.1.3	Zugriffskontrolle	10
5.1.4	Trennungskontrolle.....	11
5.1.5	Pseudonymisierung.....	11
5.2	Integrität (Art. 32 Abs. 1 lit. b DS-GVO).....	11
5.2.1	Weitergabekontrolle.....	11
5.2.2	Eingabekontrolle	12
5.3	Verfügbarkeit und Belastbarkeit.....	12
5.3.1	Verfügbarkeitskontrolle	12
5.3.2	Wiederherstellbarkeit.....	13

5.4	Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DS-GVO).....	13
5.4.1	Auftragskontrolle.....	13
6	Weiterführende Informationen	14
7	Rechtliche Hinweise / Impressum.....	14

1 Vorwort

Dieses Dokument ist als Hilfestellung für Unternehmen gedacht, die ixi-UMS Software nutzen (ab Version 6.50). Die zusammengestellten Informationen sollen die Erstellung eines Verzeichnisses der Verarbeitungstätigkeit gemäß Art. 30 Abs. 1 DSGVO erleichtern. Sie stellen keine rechtsverbindliche Auskunft dar.

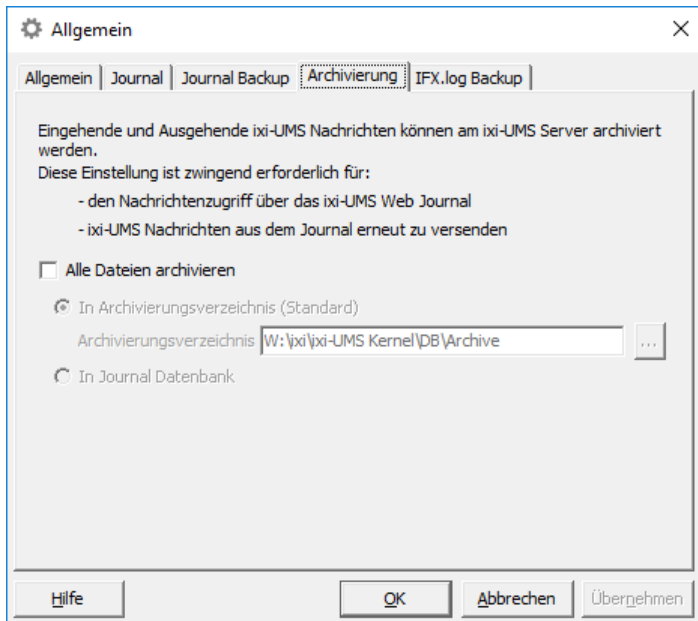
Ein solches Verzeichnis muss sämtliche der in Art. 30 Abs. 1 S. 2 lit. a bis g DSGVO abschließend genannten Angaben enthalten. Diese Angaben müssen die Verarbeitungstätigkeiten des Verantwortlichen aussagekräftig beschreiben.

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DSGVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht zu genügen. So müssen bspw. auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1 DSGVO), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1 DSGVO) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7 DSGVO) durch entsprechende Dokumentationen nachgewiesen werden.

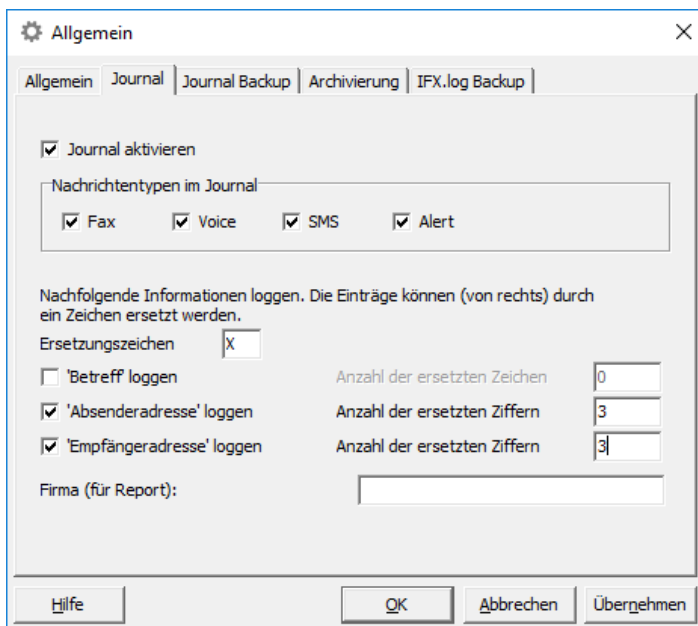
Die Kapitel sind nach Gegenstand des Verfahrens gegliedert. Jedes Kapitel enthält bereits vorausgefüllt die relevanten Informationen zu ixi-UMS ab Version 6.50.

2 Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

ixi-UMS bietet datenschutzfreundliche Voreinstellungen



ixi-UMS Enterprise bietet weitere datenschutzfreundliche Optionen



Ein-mitgeliefertes Tool ermöglicht dem Administrator gezieltes Löschen sowie Anonymisieren einzelner Journal Einträge.

3 Anlässe für ein DSGVO-Verfahren

Spätester Zeitpunkt erfasster Datensätze (Ausstellungszeitpunkt): _____

Liegt eine Auskunft, Berichtigung oder Widerspruch als Anlass vor?

- Auskunft (Art. 15 Abs. 1 DSGVO)
 - Auskunft zur Person (Verwendete Suchkriterien): <Name>, <Vorname>, <Anschrift Straße>, <Anschrift PLZ/Ort>, <Telefonnummer>, <Email-Adresse> etc.
- Berichtigung (Art. 16 DSGVO)
 - Welche Person beantragt eine Berichtigung (Verwendete Suchkriterien): <Name>, <Vorname>, <Anschrift Straße>, <Anschrift PLZ/Ort>, <Telefonnummer>, <Email-Adresse> etc.
 - Welche personenbezogenen Daten müssen geändert werden: <Name>, <Vorname>, <Anschrift Straße>, <Anschrift PLZ/Ort>, <Telefonnummer>, <Email-Adresse> etc.
- Widerspruch (Art. 21 DSGVO):
 - Löschung/Pseudonymisierung (Art. 17 DSGVO/Erwägungsgrund (ErwGr.) 26)
 - Einschränkung der Nutzung personenbezogener Daten ((Art. 18 Nr. 3 DSGVO/Erwägungsgrund (ErwGr.) 67))

4 Rechte auf Auskunft, Berichtigung oder Widerspruch der Verarbeitung

4.1 Auskunft

Die Informationen in diesem Kapitel dienen der Auskunft über die personenbezogenen Daten, welche in ixi-UMS (ab Version 6.50) verarbeitet werden.

4.1.1 Zweck und Rechtsgrundlagen der Erhebung, Verarbeitung oder Nutzung

Rechtsgrundlage §§	Aufgaben, zu deren Erfüllung die personenbezogenen Daten erhoben, verarbeitet oder genutzt werden
Auftragsverarbeitungsvertrag nach Art. 28 DSGVO	Funktionen des Produktes: Mail (M.x), Fax (F.x), Voicemail (V.x), SMS (S.x) Journal (J.x), Userverwaltung (U.x), Logs/Tracing (L.x)

4.1.2 Kategorien personenbezogener Daten, die verarbeitet werden

(mit Gruppenbezeichnungen wie Gesundheitsdaten, Bonitätsdaten usw.),

Lfd. Nr.	Bezeichnung der Daten (es reichen aussagekräftige Oberbegriffe, z. B. Namen, Anschriften; Angaben von technischen Feldern in [] (eckigen Klammern))
U.x	ixi-UserManagement:
	Titel
	Vorname
	Nachname
	Anzeige Name
	Beschreibung (beliebiger Text)
	Straße
	Postfach
	Postleitzahl
	Ort
	Staat/Bundesland

Hinweise zu Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO für ixi-UMS

	Land
	Firma
	Abteilung
	Abteilungsnummer
	Zimmer Nummer
	Mitarbeiternummer
	Telefonnummern
	Faxnummern
	Mobiltelefonnummern
	Pager Nummer
	Privat Telefonnummern
	EmailAdressen
V.	Voicemail
	UMS-Nummer des Voicemail Users
	Telefon-Nummer des Anrufers (wenn dieser nicht Rufnummern Unterdrückung aktiviert hat)
	Aufgesprochene Nachricht des Anrufers
F.	Fax
	UMS-Nummer des Fax Users
	Fax-Nummer des Anrufers (wenn dieser nicht Rufnummern Unterdrückung aktiviert hat)
	Inhalt des Faxes (also das eigentliche Fax, als TIFF oder PDF)
S.x	SMS
	UMS-Nummer des SMS-Users
	Mobil (oder Festnetz)-Nummer des SMS
	SMS Nachricht
M.1	Ankommende UMS Nachrichten als Email
	Je nach Typ Inhalte von Fax, SMS, Voice (s.o.)
	Bei aktivem Feature SenderIdentification folgende Daten aus einem MetaDirectory o.ä.
	Anzeigename
	Vorname
	Nachname
	Straße
	Postleitzahl
	Ort
	Firma
	Absender Telefonnummer
	Telefonnummer geschäftlich
	Telefonnummer mobil
	Faxnummer
	E-Mail Adresse
M.2	Als Email erzeugte ausgehende UMS Nachricht
	Je nach Typ Inhalte von Fax, SMS, Voice (s.o.)

J.x	Journal
	Rufnummer des internen Benutzers, optional, beliebige viel Stellen können aus-ge-X-t werden
	E-Mail Adresse des Benutzers
	Rufnummer des externen Teilnehmers, beliebige viel Stellen können aus-ge-X-t werden
	Betreff der Nachricht (bei ausgehenden Nachrichten Fax/Voice/SMS), optional
L.x	Logs/Trace:
	Felder aus M
	Felder aus F
	Felder aus V
	Felder aus S
	Felder aus J
	Felder aus U

4.1.3 Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung
Geplante Speicherdauer falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer.

Lfd. Nr. aus Kap. 3.1.2	Zeitraum
M.x	Keine; Nachricht befindet sich in Benutzer Mailbox, ixi-UMS hat dort keine Zugriff
F.x	Sofort nach erfolgreicher Zustellung (Maximal Versuche und Dauer sind einstellbar)
S.x	Sofort nach erfolgreicher Zustellung (Maximal Versuche und Dauer sind einstellbar)
V.x	Sofort nach erfolgreicher Zustellung (Maximal Versuche und Dauer sind einstellbar)
J.x	Keine Dauer einstellbar; Administrator kann „von Hand“ löschen
U.x	Kein automatisches Löschen vorgesehen; Administrator kann „von Hand“ löschen
T.x	Kein automatisches Löschen vorgesehen; Administrator kann „von Hand“ löschen

4.1.4 Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden

- a) lokale Benutzerverwaltung: von Hand eingetragen
- b) Benutzerverwaltung in vorhandenem Directory: aus der konfigurierten Datenquelle (z. B. Microsoft Active Directory)
- c) Kontaktdaten: aus einer einzigen konfigurierten Datenquelle (z. B. MetaDirectory)

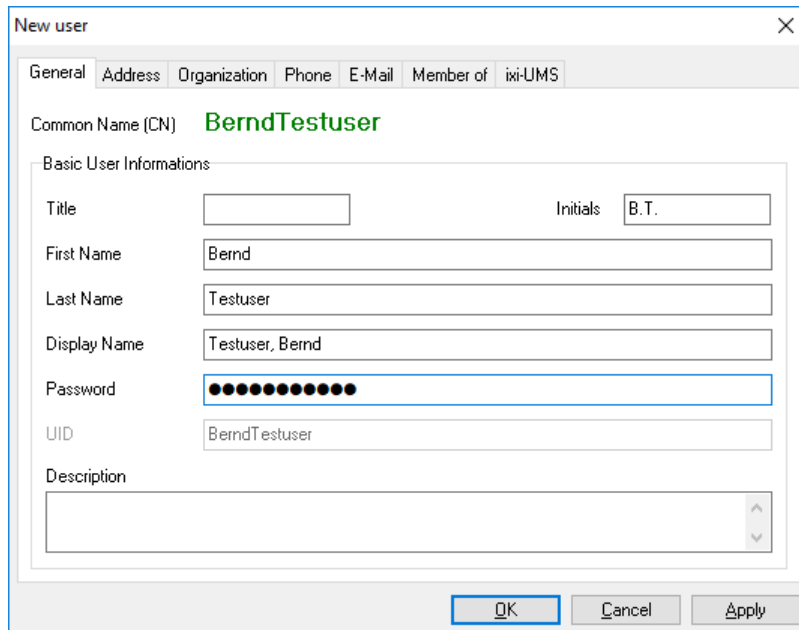
4.2 Berichtigung

Die Berechtigungsvergabe erfolgt i.d.R. durch das Berechtigungskonzept des Betriebs- und des Messaging/Groupware-Systems.

Bei lokaler Benutzer Verwaltung bietet ixi-UMS folgende Möglichkeiten

ixi-UMS Enterprise

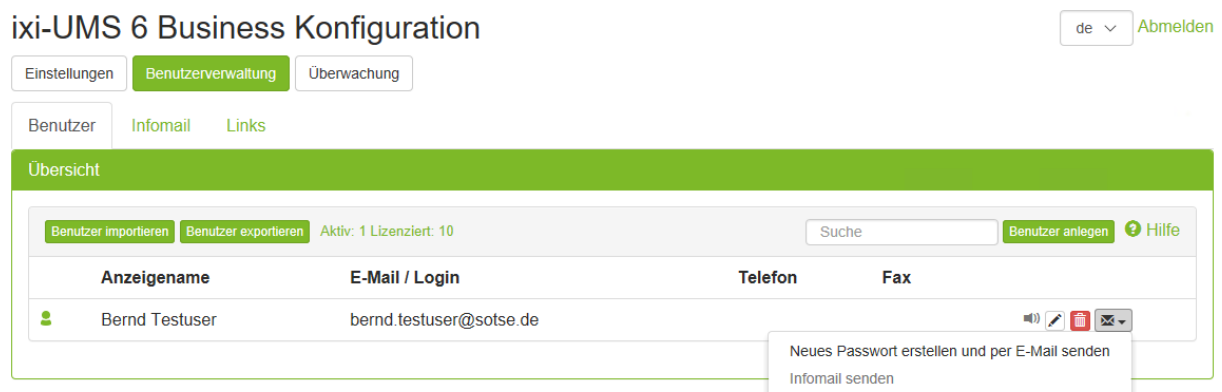
Im ixi-UMS Enterprise ist es möglich, als Administrator ein neues Passwort für die ixi-UMS spezifischen Web-Anwendungen zu vergeben.



ixi-UMS Business

Im ixi-UMS Business ist es sowohl für den Administrator als auch für Benutzer möglich, ein neues Passwort für die ixi-UMS spezifischen Web-Anwendungen zu vergeben.

ixi-UMS 6 Business Konfiguration

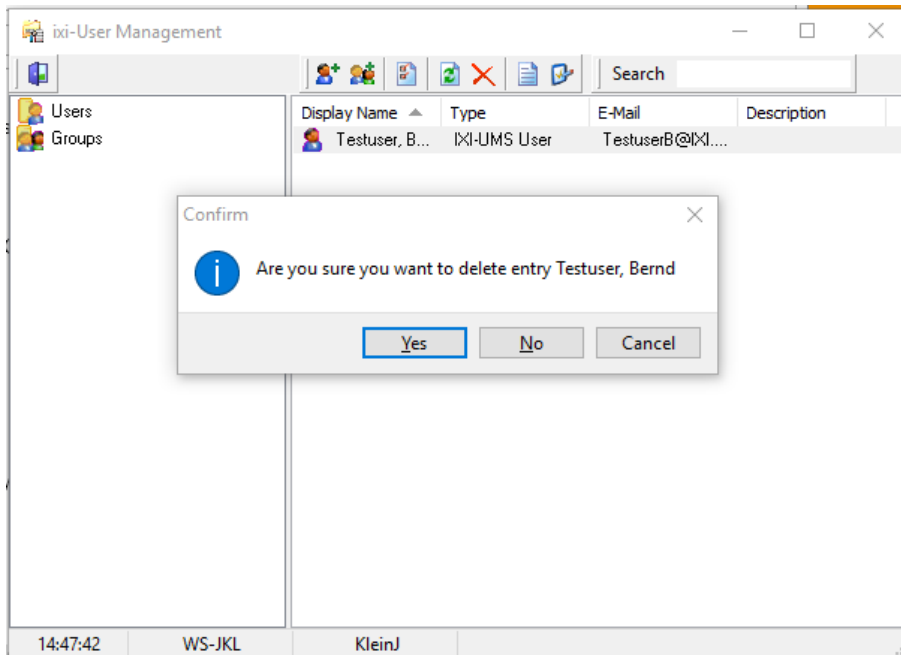


4.3 Widerspruch

4.3.1 Anonymisierung (Löschung)

ixi-UMS Enterprise

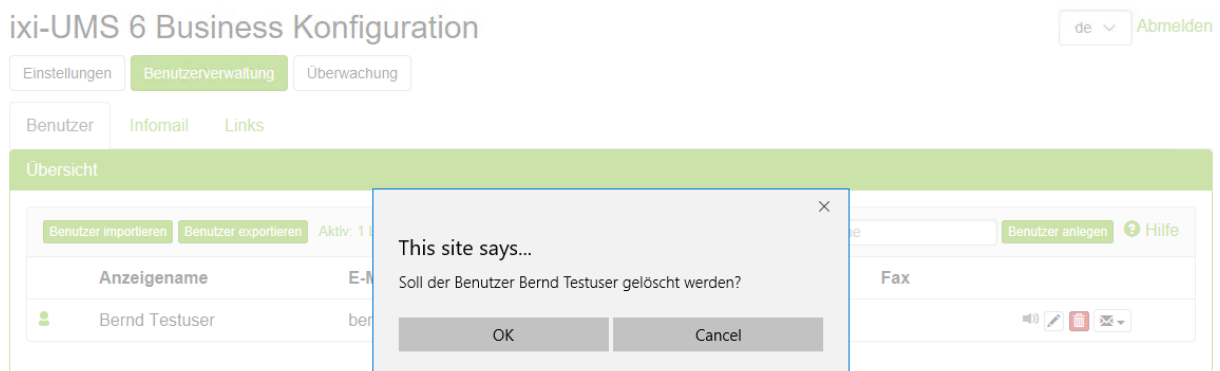
Eine Pseudonymisierung ist in ixi-UMS Enterprise derzeit nicht vorgesehen. Einzelne Benutzer können über die ixi-UMS Enterprise Konfiguration gelöscht werden.



ixi-UMS Business

Eine Pseudonymisierung ist in ixi-UMS Business derzeit nicht vorgesehen. Einzelne Benutzer können über die ixi-UMS Business Konfiguration gelöscht werden.

ixi-UMS 6 Business Konfiguration



4.3.2 Einschränkung der Verarbeitung

ixi-UMS Enterprise bietet eine Reihe von Möglichkeiten, die Verarbeitung personenbezogener Daten einzuschränken. Diese Möglichkeiten werden jetzt im Einzelnen beschrieben.

4.3.2.1 Journal

Die Daten aller Verbindungen in der Journal-Datenbank sind ausschließlich für den Administrator einsehbar.

Die SenderIdentification, also Auflösen eines Kontakts anhand der Telefon-/Fax-Nummer, ist optional.

Der einzelne Benutzer kann jeweils nur die Verbindungen für seinen eigenen Account einsehen.

Rufnummer des internen Benutzers, optional, beliebig viele Stellen können „aus-ge-X-t“ werden.

Rufnummer des externen Teilnehmers, beliebige viel Stellen können „aus-ge-X-t“ werden.

Die Speicherung des Betreffs der Nachricht (bei ausgehenden Nachrichten Fax/Voice/SMS) ist optional.

Das Journal kann komplett abgeschaltet werden.

4.3.2.2 Trace/Log

Traces und Logs sind auf Basis der Berechtigungs-Kontrolle des Betriebssystems nur für den Administrator einsehbar.

Trace/Log kann komplett abgeschaltet werden (und ist im normal betrieb i.d.R. abgeschaltet).

4.3.2.3 Mail

Die SenderIdentification, also auflösen eines Kontakts an Hand der Telefon-/Fax-Nummer) ist optional.

5 Nachweis geeigneter technischer und organisatorischer Maßnahmen nach Art. 24 Abs. 1 und Art. 32 DS-GVO

Hier werden die notwendigen Maßnahmen zur Schaffung und zum Nachweis geeigneter technischer und organisatorischer Maßnahmen nach Art. 24 Abs. 1 und Art. 32 DSGVO für die Software ixi-UMS ab Version 6.50 beschrieben.

5.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

5.1.1 Schutz vor unbefugten Zugang / Zugriffskontrollen

Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?

Der Zugang zu gespeicherten personenbezogenen Daten erfolgt über ein Administratives-Passwort zum betreffenden System, z. B. Microsoft Active Directory, LDAP-Verzeichnisdienst oder sonstigen Datenquelle wo personenbezogene Daten gespeichert werden.

Die Nutzung der ixi-UMS Verwaltung ist über das Microsoft Windows Rechteverwaltung (ixi-UMS Enterprise) bzw. ein Administrator-Passwort (ixi-UMS Business) geschützt.

Ausnahme: ixi-UMS Enterprise mit lokaler User Verwaltung

Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?

Im Rahmen der QS Tests die bei jedem Release durchgeführt werden.

Hinweise zu Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO für ixi-UMS

Ausgabestand: 17. Mai 2018

9/14

5.1.2 Zugangskontrolle

Wie erfolgt die Vergabe von Benutzerzugängen?

Durch einen Administrator, je nach Installationsvariante in der vorhandenen Benutzerverwaltung oder in der ixi-UMS lokalen Benutzerverwaltung

Wie wird die Gültigkeit von Benutzerzugängen überprüft?

Organisationsinterne Maßnahme, die durch ix-UMS nicht beeinflusst bzw. geregelt wird.

Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?

Nein; bzw. nur im Rahmen von VPN und ähnliche Methoden, die externe User in das interne Netz einbinden

5.1.3 Zugriffskontrolle

Das initiale Passwort für die ixi-UMS Web Anwendungen wird vom Administrator vergeben und kann vom Benutzer in der Web Anwendung geändert werden. Bei ixi-UMS Enterprise kann diese Option nach der Installation eingeschaltet werden

Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?

Benutzer melden sich mit Ihren Microsoft Windows-Benutzer Login an, oder über individuell eingerichtete Benutzernamen/Passwort

Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?

Ein berechtigter Administrator kann im Directory (sei dies z. B. Active Directory oder auch ixi-UMS User Verwaltung) Benutzer nach Bedarf anlegen, löschen, ändern.

Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?

Ist ixi-UMS auf Active Directory Domain verbunden/integriert, so greifen die Richtlinien (Systemeinstellungen Active Directory) zum Wechsel des Passworts.

Besteht keine Bindung zum Active Directory und es wird stattdessen die im ixi-UMS integrierte Benutzerverwaltung verwendet, besteht in ixi-UMS für den Benutzer die Möglichkeit, das Passwort über eine ixi-UMS Web Anwendung zu ändern; bei ixi-UMS Enterprise kann diese Möglichkeit ein- und ausgeschaltet werden.

Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird

Wie erfolgt die Dokumentation von Zugriffsberechtigungen?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie lange werden Protokolle aufbewahrt?

Siehe 4.1.3 Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung

Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?

Zugriff auf die Protokolle hat nur der Administrator des Systems; teils abgesichert durch ixi-UMS selbst teils abgesichert durch Berechtigungsvergabe seitens des Betriebssystems

5.1.4 Trennungskontrolle

Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

5.1.5 Pseudonymisierung

Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?

Außer im Journal werden keine Personenbezogenen Daten aufbewahrt/gespeichert; mögliche Anonymisierungs-Möglichkeiten beim Journal sind in 4.1.2 „aus-x-en“ aufgezeigt.

5.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

5.2.1 Weitergabekontrolle

Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie wird die Weitergabe personenbezogener Daten dokumentiert?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

5.2.2 Eingabekontrolle

Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?

Für die ixi-UMS Webanwendungen kann durch ixi-UMS eine Protokollierung (Log) der Anmeldung und Abmeldung sowie die durchgeführten Aktionen für alle User erfolgen.

Es gilt 4.1.3 Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung

Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

5.3 Verfügbarkeit und Belastbarkeit

5.3.1 Verfügbarkeitskontrolle

Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?

Die Software ixi-UMS ist signiert, d.h. Änderungen an der Anwendung würden die Signatur verletzen und so eine Manipulation aufdecken.

Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

5.3.2 Wiederherstellbarkeit

Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?

(rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)

ixi-UMS kann im Cluster Betrieb voll-redundant implementiert werden. Speicherung der wenigen persistenten Dateien wie z. B. das Journal kann ein RAID/NAS System sein.

5.4 Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)

Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?

Die Basisinstallation von ixi-UMS enthält keine personenbezogenen Daten.

Personenbezogene Daten können über folgende Wege ins Produkt gelangen:

- Lokale User Verwaltung; Voreinstellung ist Nutzung vorhandener User Verwaltung wie z. B. Active Directory
Bei Fax/SMS/Voice Versand entstehen Journal Daten; Das Journal kann komplett abgeschaltet werden, Telefonnummern können teilweise oder ganz „aus ge-X-t“ werden.

5.4.1 Auftragskontrolle

Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?

Organisationsinterne Maßnahme, die durch ixi-UMS nicht beeinflusst bzw. geregelt wird.

6 Weiterführende Informationen

Weiterführende Informationen über estos z. B. zu unseren Produkten, Dienstleistungen, Datenschutzrichtlinien, Verhaltenskodex erhalten Sie auf unserer Webseite www.estos.de bzw. www.estos.com

7 Rechtliche Hinweise / Impressum

Die Angaben in diesem Dokument entsprechen dem Kenntnisstand zum Zeitpunkt der Erstellung. Irrtümer und spätere Änderungen sind vorbehalten.

Die estos GmbH schließt jegliche Haftung für Schäden aus, die direkt oder indirekt aus der Verwendung dieses Dokumentes entstehen.

Genannte Marken- und Produktbezeichnungen sind Warenzeichen oder Eigentum der entsprechenden Inhaber.

Copyright estos GmbH. Alle Rechte vorbehalten.

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

info@estos.de

www.estos.de