

Technische und organisatorische Maßnahmen (TOM) – Sicherheit der Verarbeitung gem. Artikel 32 DSGVO

A. Vertraulichkeit

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Umgesetzte Maßnahmen

Die Geschäftsräume der windata GmbH befinden sich im Weißgerberweg 11, 88239 Wangen im Allgäu.

a) Alarmanlage

Überprüfung: mind. 1-mal jährlich durch externen, zertifizierten Dienstleister

b) Automatisiertes Zugangskontrollsystem

Zugangskarten mit Berechtigungskonzept

Überprüfung: durch DSB

c) Lichtschranken/Bewegungsmelder

In den Eingangsbereichen sind Bewegungsmelder installiert, die bei Dunkelheit aktiv sind und den unbemerkten Zugang zum Gebäude über den vorhandenen Zugang zu unseren Geschäftsräumen erschweren

d) Schließsystem, Schlüsselausgabe und -kontrolle

Die Ausgabe der Schlüssel (elektronischer Schlüssel-Batch) wird von der windata GmbH verwaltet und kontrolliert. Den Notschlüssel verwaltet der Geschäftsführer.

Überprüfung: mind. 1-mal jährlich durch DSB windata

e) Personenkontrolle beim Empfang und Protokollierung der Besucher

Nicht autorisierte Personen erhalten Zugang zu den Geschäftsräumen nur nach vorheriger Anmeldung am Empfang. Es findet eine Protokollierung des Zugangs in schriftlicher Form (Besuchermanmeldung) statt. Das ordnungsgemäße Verlassen der Geschäftsräume wird ebenfalls protokolliert.

Zuständigkeit: windata GmbH, Empfang

Überprüfung: Stichprobenhafte Kontrolle der Protokolle in unregelmäßigen Zeitabständen durch die DSB

f) Auswahl von Reinigungspersonal

Es wird kein externes Dienstleistungsunternehmen mit der Reinigung der Büroräume beauftragt. Reinigungspersonal ist angestellt bei der windata GmbH und unterliegt der allgemeinen Geheimhaltung gem. Anstellungsvertrag

Zuständigkeit: windata GmbH, Personalleitung

g) Aufschaltung des Wachdienstes

Derzeit findet eine Überwachung des Gebäudes durch Aufschaltung des Wachdienstes statt bei: Einbruchversuch, Feuerausbruch, Überhitzung des Serverraumes, offenen Fenstern und Türen nach Einschaltung der Anlage.

Zuständigkeit: windata GmbH

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Umgesetzte Maßnahmen

a) Zuordnung von Benutzerprofilen

gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

b) Erstellen von Benutzerprofilen

gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

c) Richtlinien für die Passwortvergabe

gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

d) Zuordnung von Benutzerprofilen zu IT-Systemen

gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

e) Einsatz von VPN-Technologie

Die eingesetzte VPN-Technologie nutzt eine 256 Bit AES-Verschlüsselung. Die jeweiligen VPN-Profilen sind individuell für die einzelnen Nutzer generiert und können nur mit einer MFA (Authenticator-APP) genutzt werden.

Hersteller: SOPHOS

Modell: SOPHOS ConnectClient v2

Zuständigkeit: windata GmbH, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

f) Sicherheitsschlösser und Schlüsselausgabe

Der Zugang zu den Räumlichkeiten des zentralen Datenverarbeitungssystems (Serverraum) ist durch ein elektronisches Sicherheitsschloss gesichert und nur einem bestimmten ausgewählten Personenkreis zugänglich.

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

g) Personenkontrolle beim Empfang und Protokollierung der Besucher

Nichtautorisierte Personen erhalten keinen alleinigen Zugang zum Serverraum. Bei Bedarf eines Zugangs zum Serverraum durch Dritte (z.B. Servicetechniker, Wartungsarbeiten, Handwerker etc.) ist immer eine autorisierte Person zur Überwachung anwesend.

Überprüfung: mind. 1-mal jährlich durch DSB windata

h) Auswahl von Reinigungspersonal

Das Reinigungspersonal hat keinen Zutritt zum Serverraum. Notwendige Reinigungsarbeiten werden nur bei Anwesenheit einer autorisierten Person durchgeführt.

Überprüfung: mind. 1-mal jährlich durch DSB windata

i) Aufschaltung des Wachdienstes

Der Wachdienst schaltet sich im Bedarfsfall auf (Einbruch, Feuer, Überhitzung vom Serverraum, offene Fenster/Türen etc.).

Zuständig: Eckert Sicherheitstechnik, Friedrichshafen, windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

j) Firewall, Intrusion-Detection-System (IDS) und Anti-Viren-Software

Es werden mehrere Systeme in jeweils der vom Hersteller bereitgestellten aktuellen und vom Administrator zur Verwendung geprüften und freigegebenen Version kombiniert eingesetzt.

Überprüfung: mind. 1-mal jährlich durch DSB windata

- Firewall (Router/Gateway)

Hersteller: SOPHOS

- Firewall (Server/Arbeitsplatzrechner)

Hersteller: Microsoft

- Route/Gateway (IDS)

Hersteller: SOPHOS

- Serversysteme (Anti-Viren)

Hersteller: Microsoft

- Arbeitsplatzsystem und mobile Geräte (Anti-Viren)

Hersteller: Microsoft

3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Umgesetzte Maßnahmen

a) Berechtigungskonzept

gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

b) Verwaltung der Rechte durch Systemadministration

gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“. Die Anzahl der Benutzer mit administrativen Berechtigungen ist auf die betriebliche Notwendige reduziert.

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

c) Richtlinien für die Passwortvergabe

gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

d) Sichere Aufbewahrung von Datenträgern

gem. der „Richtlinie für Datenträger“

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

e) Verschlüsselung mobiler Datenträger und Datenträgern in Laptops/Notebooks, Aufbewahrung mobiler Datenträger

Mobile Datenträger (externe Festplatten, USB-Sticks etc.) werden gem. der „Richtlinie für Datenträger“ behandelt.

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

f) Löschung und Vernichtung von Datenträgern und Akten

gem. der „Richtlinie für Datenträger“. Die Vernichtung wird protokolliert.

Zuständigkeit: windata GmbH, Geschäftsführung, BackOffice

Überprüfung: mind. 1-mal jährlich durch DSB windata

Als externer Dienstleister für die physikalische Vernichtung von Akten und Datenträgern wurde die, für die Datenvernichtung nach DIN 32757 zertifizierte Evangelische Heimstiftung GmbH (Stephanuswerk Isny), WfbM - Außenstelle Leutkirch, Nadlerstraße 21, 88299 Leutkirch beauftragt.

4. Trennungsgebot und Pseudonymisierung

Es sind Maßnahmen zu treffen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umgesetzte Maßnahmen

a) Physikalische Trennung auf gesonderten Systemen

Systeme mit Anwendungen/Applikationen werden, sofern vom Hersteller der Software ermöglicht, getrennt von den Datenbeständen (Mandantentrennung in Datenbanken) auf eigenständigen und abgesicherten Systemen gehalten.

Hierzu wird Virtualisierungstechnologie in der jeweils vom Hersteller aktuellen und vom Administrator geprüften und freigegebenen Version eingesetzt. Alle Aktivitäten der Systeme werden protokolliert. Der technische Zugriff auf die Systeme ist durch eine interne Verhaltensrichtlinie und die Zugriffsrechte der Benutzer sind gem. der „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“ geregelt.

Hersteller: Microsoft

Zuständigkeit: windata GmbH, Entwicklung, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

b) Trennung von Produktiv- und Testsystemen

Produktiv- und Testsysteme sind durch technische Mittel (Sophos) oder durch virtuelle Netze (VLAN) getrennt.

Zuständigkeit: windata GmbH, Entwicklung, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

c) Pseudonymisierung (Produkte)

Eigene (selbstentwickelte) Softwareprogramme wurden angepasst, um Pseudonymisierung gem. der DSGVO zu gewährleisten

Zuständigkeit: windata GmbH, Entwicklung, Geschäftsführung

Überprüfung: Vor Release Freigabe durch DSB windata

d) Prozesse zur Wahrung von Betroffenenrechten

gem. interner Richtlinie und Prozesse; Checklisten; Formulare

Zuständigkeit: windata GmbH, Geschäftsführung, DSB windata

Überprüfung: Umgehend nach Durchführung durch DSB windata

e) Software-Updates

Aktualisierung der eingesetzten Softwareprogramme zur Verarbeitung von Kundendaten, sobald DSGVO-konforme Versionen von den Herstellern bereitgestellt werden

Zuständigkeit: windata GmbH, Entwicklung, Geschäftsführung

B Integrität

1. Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Umgesetzte Maßnahmen

a) Standleitungen und VPN-Tunnel

Die Anbindung an das Internet - auch für die Telefonie (VoIP) - ist durch eine 500/50 Mbit Vodafone COAX ADSL sichergestellt bzw. mit einer ausfallsicheren Leitung: 200/20 Mbit/s vom Betreiber: Telekom Deutschland

Zuständigkeit: Vodafone, Administrator

Fallback: DSL, Telekom Deutschland

Überprüfung: mind. 1-mal jährlich durch DSB windata

b) E-Mailkonten

Als Mailserver verwenden wir einen Exchange Online (Microsoft 365) - siehe „Richtlinie für E-Mail“. Die Mailkommunikation ist nach aktuellen Standards verschlüsselt. Ein- und ausgehende E-Mails werden vom System protokolliert. Hersteller: Microsoft

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

c) Protokollierung

Aktivitäten der Serversysteme und Zugriffe auf diese Systeme werden protokolliert und regelmäßig vom Administrator geprüft und überwacht.

Überprüfung: mind. 1-mal jährlich durch DSB windata

d) Physischer Transport von Datenträgern

gem. der „Richtlinie für Datenträger“

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

2. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Umgesetzte Maßnahmen

a) Protokollierung

Protokollierung der Eingabe, Änderung und Löschung von Daten im Datensystem gem. interner „Richtlinie für Informations- und Kommunikationstechnik (IuK)“

Überprüfung: mind. 1-mal jährlich durch DSB windata

b) Nachvollziehbarkeit

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“

Überprüfung: mind. 1-mal jährlich durch DSB windata

c) Aufbewahrung

Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind gem. interner „Richtlinie für Informations- und Kommunikationstechnik (IuK)“

Überprüfung: mind. 1-mal jährlich durch DSB windata

d) Vergabe von Rechten

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts gem. interner „Richtlinie für Benutzerkonten, Benutzerrechte und Passwörter“

Überprüfung: mind. 1-mal jährlich durch DSB windata

3. Zweckbindungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umgesetzte Maßnahmen

a) Serielle Verarbeitung von Kundendaten

getrennt nach Kundin/Kunde und Auftrag

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 2-mal jährlich durch DSB windata

b) Verschiedene Softwareprogramme

nach Art und Zweck der Daten getrennte Verarbeitung

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich bzw. nach Releasewechsel durch DSB windata

c) Mandantentrennung

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

4. Weisungskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Umgesetzte Maßnahmen

a) Vertragliche Vereinbarungen

Vertrag zur Auftragsverarbeitung gem. Artikel 28 Abs. 3 DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

b) Kompetenz- und Zuständigkeitsregelungen

Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

c) Kontrolle und Überprüfung

weisungsgebundener Auftragsdurchführung

Zuständigkeit: windata GmbH, Geschäftsführung,

Überprüfung: mind. 1-mal jährlich durch DSB windata

d) Verpflichtung der Mitarbeiter zur Vertraulichkeit

über Anstellungsvertrag und zusätzliche, tätigkeitsbezogene Vertraulichkeitsvereinbarung

Zuständigkeit: windata GmbH, Geschäftsführung,

Überprüfung: mind. 1-mal jährlich durch DSB windata

e) Richtlinien und Vorgaben

Interne Richtlinien zum Umgang mit Informations- und Kommunikationstechnik (IuK), Datenträgern, Benutzerkonten, Benutzerrechten und Passwörter sowie E- Mails

Zuständigkeit: windata GmbH, Geschäftsführung,

Überprüfung: mind. 2-mal jährlich durch DSB windata

f) Datenschutzbeauftragte

Benennung einer/s Beauftragten für den Datenschutz (gem. Artikel 37 ff. DSGVO) und einer Stellvertretung

Zuständigkeit: windata GmbH, Geschäftsführung

g) Verarbeitungsverzeichnis

Führen eines Verzeichnisses der Verarbeitungstätigkeiten gem. Artikel 30 Abs. 2 DSGVO

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

C Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung, bei hoher Beanspruchung oder Verlust geschützt sind.

Umgesetzte Maßnahmen

a) Unterbrechungsfreie Stromversorgung

Die zentralen Datenverarbeitungssysteme sind durch eine unterbrechungsfreie Stromversorgung (USV) abgesichert.

Hersteller: APC, Version APC-SRT5KRMXLI

Zuständigkeit: windata GmbH, Administrator

Überprüfung: mind. 2-mal jährlich durch DSB windata

b) Klimaanlage und Temperaturüberwachung

Die zentralen Datenverarbeitungssysteme sind durch eine Klimaanlage vor Überhitzung gesichert. Es findet eine mindestens jährliche Überprüfung der Klimaanlage durch das Fachunternehmen Kälte Fritz, Hergensweiler statt.

Zuständigkeit: windata GmbH, Eckert Sicherheitstechnik, Friedrichshafen

Überprüfung: mind. 1-mal jährlich durch zertifiziertes Fachunternehmen

c) Brandmeldeanlage

Die zentralen Datenverarbeitungssysteme sind durch eine Brandmeldeanlage (Feuermelder) gesichert.

Zuständigkeit: windata GmbH, Eckert Sicherheitstechnik, Friedrichshafen

Überprüfung: mind. 1-mal jährlich durch zertifiziertes Fachunternehmen

d) Feuerlöschgeräte

Im Raum der zentralen Datenverarbeitungsanlage ist ein Feuerlöschgerät installiert.

Zuständigkeit: windata GmbH, Brandschutzbeauftragter

Überprüfung: mind. 1-mal jährlich durch Brandschutzbeauftragten der windata

e) Datensicherung und Datenwiederherstellung

Automatische Datensicherungen (20:00 Uhr bis 5:00 Uhr) aller Serversysteme auf getrennten Systemen mit aktuellen und vom Administrator geprüften und freigegebenen Backuplösungen gem. Richtlinie „Datensicherung und Datenrücksicherung“. Die Funktion der Backuplösung wird vom Administrator (mittels Monitoring) täglich geprüft, kontrolliert und protokolliert. Eine Datenwiederherstellung erfolgt im Falle eines Systemfehlers oder bei Defekt von Hardware auf einem neu installierten und geprüften System.

Hersteller: Synology Active Backup for business

Zuständigkeit: windata GmbH, Geschäftsführung, Administrator

Überprüfung: mind. 1-mal jährlich durch DSB windata

f) Notfallplan

Ein Notfallplan für interne IT-Systeme ist vorhanden.

Zuständigkeit: windata GmbH, Administration, Geschäftsführung

D. Bewertung und Evaluierung

1. Datenschutz-Maßnahmen

Es werden regelmäßig vom externen Datenschutzbeauftragten der windata GmbH Datenschutzprüfungen und Schulungen der Mitarbeiter durchgeführt. Die Mitarbeiter werden auf Vertraulichkeit verpflichtet.

Auf eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz haben alle Mitarbeiter nach Bedarf Zugriff.

2. Incident-Response-Management

Das Incident-Response-Management unterstützt bei der Reaktion auf Sicherheitsverletzungen.

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virens Scanner und regelmäßige Aktualisierung
- Einsatz von Intrusion Detection System
- Einsatz von Intrusion Prevention System

Organisatorisch wird dies vollzogen durch eine dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen, der Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem und deren Nachbereitung.

3. Privacy by Design und Privacy by Default

Datenschutzfreundliche Voreinstellungen sind getroffen, indem nicht mehr personenbezogene Daten als für den jeweiligen Zweck erforderlich erhoben werden.

Die windata GmbH pflegt eine einfache Ausübung des Widerrufsrechts eines Betroffenen und regelgetreue Löschung.

4. Auftragskontrolle

Es ist zu gewährleisten, dass der Auftragnehmer den Auftraggeber bei der Durchführung der im Vertrag geregelten Kontrollen unterstützt.

Umgesetzte Maßnahmen

a) Auswahl, Prüfung von Auftragnehmern und Weisungen

Alle Auftragnehmer der windata GmbH werden unter Sorgfaltsgesichtspunkten ausgewählt und auf die Einhaltung des Datenschutzes gem. DSGVO verpflichtet.

Zuständigkeit: windata GmbH, Geschäftsführung

Überprüfung: vor Auftragsvergabe Prüfung durch DSB windata

b) Vertragliche Vereinbarungen

Vertrag zur Auftragsverarbeitung gem. Artikel 28 Abs. 3 DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen. Hierzu werden vertragliche Regelungen („Vertrag zur Auftragsverarbeitung“) zwischen Auftragnehmer und der windata GmbH getroffen. Von Auftragnehmern werden die technischen und organisatorischen Maßnahmen (TOM) und deren strikte Einhaltung eingefordert. Nach Risikoeinschätzung werden vom Auftragnehmer erweiterte Versicherungen (Zertifikate, Audits oder Stellungnahmen) eingefordert. Der Auftragnehmer hat sicherzustellen, dass auch dessen Mitarbeiter auf die Einhaltung des Datengeheimnisses verpflichtet werden. Bei hohem Sicherheitsrisiko werden vertraglich Sanktionen und Strafen für den Fall von Vertragsverstößen vereinbart.

Zuständigkeit: windata GmbH, Datenschutzbeauftragte und Geschäftsführung

Überprüfung: min. 1-mal jährlich durch DSB windata

c) Sicherstellung der Datenvernichtung nach Beendigung des Auftrags

gem. Richtlinie „Allgemeine Verhaltensregeln für den Umgang mit personenbezogenen Daten“

Zuständigkeit: windata GmbH, Datenschutzbeauftragte und Geschäftsführung

Überprüfung: mind. 1-mal jährlich durch DSB windata

d) Laufende Überprüfung von Auftragnehmern

Verträge mit Auftragnehmern werden befristet geschlossen. Vor einer Verlängerung des Vertragsverhältnisses erfolgt eine erneute Überprüfung des Auftragnehmers gem. D 4. a).

Zuständigkeit: windata GmbH, Datenschutzbeauftragte und Geschäftsführung

Überprüfung: min. 1-mal jährlich durch DSB windata

Freigegeben zur Veröffentlichung Mai 2025

Michael Rudhart
Geschäftsführer

windata GmbH
Weißgerberweg 11
88239 Wangen im Allgäu
Telefon +49 7522 9770-0
Email info-wangen@cisbox.com

Geschäftsführer: Michael Rudhart, Christof Majer

Handelsregister Ulm HRB 721386
Umsatzsteuer-ID DE445876474

Beauftragte für den Datenschutz: SICDATA - Unternehmensberatung
Tobias Erdmann, Heiligenstock 34d, 42697 Solingen;
MA stv. Beauftragte für den Datenschutz: datenschutz-wangen@cisbox.com