Technische und organisatorische Maßnahmen (TOM) - erweiterte Erläuterungen, Sicherstellung der Einhaltung und Sicherheit der Verarbeitung gem. Artikel 32 DSGVO

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 & Co.KG befinden sich im Gebäude der Kreissparkasse Ravensburg, Geschäftsstelle Wangen im Allgäu. Die Kreissparkasse Ravensburg stellt diverse Sicherheitseinrichtungen zur Zutrittskontrolle im Rahmen des bestehenden Mietvertrages und garantiert deren Überwachung, Kontrolle und Funktion. Die Kreissparkasse Ravensburg garantiert gegenüber der windata GmbH & Co.KG die Einhaltung der notwendigen Wartung und Betriebssicherheit.

a. Alarmanlage
Hersteller: BOSCH Sicherheitssysteme
Prüfung: Vierteljährlich durch BOSCH Sicherheitssysteme, Prüfung wird in einem Wartungsbuch eingetragen
Zuständigkeit: Kreissparkasse Ravensburg
Überprüfung: mind. 1 Mal jährlich durch externen, zertifizierten Dienstleister

b. Absicherung von Gebäudeschächten
Zuständigkeit: Kreissparkasse Ravensburg
Überprüfung: mehrmals jährlich

c. Automatisiertes Zugangskontrollsystem
Hersteller: INFORM Solutions
Erstellung der Zugangskarten: Berechtigungskonzept der Kreissparkasse Ravensburg Zuständigkeit: Kreissparkasse Ravensburg
Überprüfung: Überprüfung durch DSB der Kreissparkasse Ravensburg

d. Videoüberwachung
Der Haupteingang (Foyer) zum Gesamtgebäude wird mittels Video überwacht. Nebeneingänge werden nicht überwacht.
Zuständigkeit: Kreissparkasse Ravensburg
Überprüfung: mind. 1 Mal jährlich durch externen, zertifizierten Dienstleister

e. 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
Zuständigkeit: Kreissparkasse Ravensburg

f. Schließsystem, Schlüsselausgabe und -kontrolle
Hersteller: KABA
Die Ausgabe der Schlüssel (Schlüssel-Management) wird von der Kreissparkasse Ravensburg verwaltet und kontrolliert
Zuständigkeit: Kreissparkasse Ravensburg
Überprüfung: mind. 1 Mal jährlich durch DSB windata

g. Personenkontrolle beim Empfang und Protokollierung der Besucher
Nicht autorisierte Personen erhalten Zugang zu den Geschäftsräumen nur nach vor-heriger Anmeldung am Empfang. Es findet eine Protokollierung des Zugangs in schriftlicher Form (Besucheranmeldung) statt. Das ordnungsgemäße Verlassen der Geschäftsräume wird protokolliert.
Zuständigkeit: windata GmbH & Co.KG, Empfang
Überprüfung: Stichprobenhafte Kontrolle der Protokolle in unregelmäßigen Zeitab-ständen durch die DSB

h. Auswahl von Reinigungspersonal
Es wird kein externes Dienstleistungsunternehmen mit der Reinigung der Büroräume beauftragt. Reinigungspersonal ist angestellt bei der windata GmbH & Co.KG und un-terliegt der allgemeinen Geheimhaltung gem. Anstellungsvertrag
Zuständigkeit: windata GmbH & Co.KG, Personal

i. Auswahl von Wachpersonal
Derzeit wird kein Wachpersonal beschäftigt bzw. es ist kein externer Dienstleister mit der Überwachung beauftragt.

2. Zugangskontrolle

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

Umgesetzte Maßnahmen

a. Zuordnung von Benutzerprofilen
gem. interner „Richtline für Benutzerkonten, Benutzerrechte und Passwörter"
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

b. Erstellen von Benutzerprofilen
gem. interner „Richtline für Benutzerkonten, Benutzerrechte und Passwörter"
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

c. Richtlinien für die Passwortvergabe
gem. interner „Richtline für Benutzerkonten, Benutzerrechte und Passwörter"
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

d. Zuordnung von Benutzerprofilen zu IT-Systemen
gem. interner „Richtline für Benutzerkonten, Benutzerrechte und Passwörter"
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

e. Einsatz von VPN-Technologie
Die eingesetzte VPN-Technologie nutzt eine 256 Bit AES-Verschlüsselung mittels ei-ner (hardwarebasierten) Sophos Red-Box. Die Ausgabe der Red-Box wird durch den Administrator verwaltet, kontrolliert und protokolliert
Hersteller: SOPHOS
Model: RED
Zuständigkeit: windata GmbH & Co.KG, Administration
Überprüfung: mind. 1 Mal jährlich durch DSB windata

f. Sicherheitsschlösser und Schlüsselausgabe
Der Zugang zu den Räumlichkeiten des zentralen Datenverarbeitungssystems (Serverraum) ist durch ein Sicherheitsschloss gesichert. Es existieren zwei Schlüssel, die getrennt von den zutrittsberechtigten Personen verwahrt werden. Derzeit verwahrt ein Schlüssel der Systemadministrator und ein Schlüssel die DSB
Hersteller: KABA
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

g. Personenkontrolle beim Empfang und Protokollierung der Besucher
Nicht-autorisierte Personen erhalten keinen alleinigen Zugang zum Serverraum. Bei Bedarf eines Zugangs zum Serverraum durch Dritte (z.B. Servicetechniker, Wartungs-arbeiten, 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. Auswahl von Wachpersonal
Es besteht derzeit kein Bedarf für Wachpersonal des zentralen Datenverarbeitungssystems

j. Firewall, Intrusion-Detection-System (IDS) und Anti-Viren-Software
Es werden mehre System in jeweils der vom Hersteller bereitgestellten aktuellen und vom Administrator zur Verwendung geprüften und freigegeben Version kombiniert eingesetzt.
Überprüfung: mind. 1 Mal jährlich durch DSB windata

- **i.** Firewall (Router/Gateway)
  Hersteller: SOPHOS
- **ii.** Firewall (Server/Arbeitsplatzrechner)
  Hersteller: ESET und betriebssystemeigene (Microsoft)
- **iii.** Route/Gateway (IDS)
  Hersteller: SOPHOS
- **iv.** Serversysteme (Anti-Viren)
  Hersteller: ESET
- **v.** Arbeitsplatzsystem und mobile Geräte (Anti-Viren)
  Hersteller: ESET

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 „Richtline für Benutzerkonten, Benutzerrechte und Passwörter"
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

b. Verwaltung der Rechte durch Systemadministration
gem. interner „Richtline für Benutzerkonten, Benutzerrechte und Passwörter". Die Anzahl der Benutzer mit administrativen Berechtigungen ist auf das betrieblich Notwendige reduziert.
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

c. Richtlinien für die Passwortvergabe
gem. interner „Richtline für Benutzerkonten, Benutzerrechte und Passwörter"
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

d. Sichere Aufbewahrung von Datenträgern
gem. der „Richtline für Datenträger"
Zuständigkeit: windata GmbH & Co.KG, Administration und 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 „Richtline für Datenträger" behandelt.
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

f. Löschung und Vernichtung von Datenträgern und Akten
gem. der „Richtline für Datenträger". Die Vernichtung wird protokolliert.
Zuständigkeit: windata GmbH & Co.KG, Administration, BackOffice und Geschäftsführung
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, Nadler-straße 21, 88299 Leutkirch beauftragt.

4. 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 1GB Glasfaserverkabelung hergestellt.
Betreiber: Telekommunikation Lindau (B) GmbH, Auenstraße 12, 88131 Lindau
Zertifikate: TÜViT Level3
Zuständigkeit: Telekommunikation Lindau (B) GmbH, Administration
Fallback: Koaxialverbindung, Unitymedia Business
Überprüfung: mind. 1 Mal jährlich durch DSB windata

b. E-Mailkonten
Es bestehen zentrale (unternehmensübergreifende) und persönliche E-Mailkonten gem. „Richtline für E-Mail". Ein- und ausgehende E-Mails werden über ein eigenes, intern betriebenes Mailsystem über das SMTPS-Protokoll mit TLS/SSL-Authentifizie-rung abgewickelt. Es besteht ein SSL-Zertifikat für den Mailserver. Ein- und ausgehende E-Mails werden vom System protokolliert.
Hersteller: Microsoft
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Zertifizierungsstelle: GeoTrust
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 „Richtline für Datenträger"
Zuständigkeit: windata GmbH & Co.KG, Administration und Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

5. 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 der Eingabe, Änderung und Löschung von Daten
gem. interner „Richtline für Informations- und Kommunikationstechnik (IuK)"
Überprüfung: mind. 1 Mal jährlich durch DSB windata

b. Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
gem. interner „Richtline für Informations- und Kommunikationstechnik (IuK)"
Überprüfung: mind. 1 Mal jährlich durch DSB windata

c. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch indivi-duelle Benutzernamen (nicht Benutzergruppen)
gem. interner „Richtline für Benutzerkonten, Benutzerrechte und Passwörter"
Überprüfung: mind. 1 Mal jährlich durch DSB windata

d. Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitun-gen übernommen worden sind
gem. interner „Richtline für Informations- und Kommunikationstechnik (IuK)"
Überprüfung: mind. 1 Mal jährlich durch DSB windata

e. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
gem. interner „Richtline für Benutzerkonten, Benutzerrechte und Passwörter"
Überprüfung: mind. 1 Mal jährlich durch DSB windata

6. 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 & Co.KG werden unter Sorgfaltsgesichtspunk-ten ausgewählt und auf die Einhaltung des Datenschutzes gem. DSGVO verpflichtet. Zuständigkeit: windata GmbH & Co.KG, 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 & Co.KG getroffen. Von Auftragnehmern werden die technischen und organisatorischen Maßnahmen (TOM) und deren strikte Einhal-tung eingefordert. Nach Risikoeinschätzung werden vom Auftragnehmer erweiterte Versicherungen (Zertifikate, Audits oder Stellungnahmen) eingefordert. Der Auftragnehmer hat sicherzustellen, dass auch dessen Mitarbeiter_innen auf die Einhaltung des Datengeheimnisses verpflichtet werden. Bei hohem Sicherheitsrisiko werden vertraglich Sanktionen und Strafen für den Fall von Vertragsverstößen vereinbart. Zuständigkeit: windata GmbH & Co.KG, Datenschutzbeauftragte und Geschäftsführung
Überprüfung: mind. 4 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 & Co.KG, Datenschutzbeauftragte und Geschäftsführung
Überprüfung: mind. 4 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. 6. a.
Zuständigkeit: windata GmbH & Co.KG, Datenschutzbeauftragte und Geschäftsfüh-rung
Überprüfung: mind. 2 Mal jährlich durch DSB windata

7. Verfügbarkeitskontrolle

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

Umgesetzte Maßnahmen

a. Unterbrechungsfreie Stromversorgung
Die zentralen Datenverarbeitungssysteme sind durch eine unterbrechungsfreie Stromversorgung (USV) abgesichert.
Hersteller: APC, Version APCSMT2200I
Zuständigkeit: windata GmbH & Co.KG, Administration
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 Kältetechnik Harrer, Richthofenstraße 7, 88239 Wangen statt.
Zuständigkeit: windata GmbH & Co.KG, Administration
Überprüfung: mind. 1 Mal jährlich durch zertifiziertes Fachunternehmen

c. Brandmeldeanlage
Die zentralen Datenverarbeitungssysteme sind durch eine Brandmeldeanlage (Feuer-melder) gesichert.
Zuständigkeit: windata GmbH & Co.KG, Administration
Überprüfung: mind. 1 Mal jährlich durch zertifiziertes Fachunternehmen

d. Feuerlöschgeräte
Im Raum der zentralen Datenverarbeitungsanlage ist ein Feuerlöschgerät installiert. Zuständigkeit: windata GmbH & Co.KG, Brandschutzbeauftragter
Überprüfung: mind. 1 Mal jährlich durch Brandschutzbeauftragten der windata

e. Datensicherung und Datenwiederherstellung
Automatische Datensicherungen (jeweils um 20:00 Uhr und um 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: Altaro und DSM HyperBackup
Zuständigkeit: windata GmbH & Co.KG, Administration, Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

f. Notfallplan
Der bestehende Notfallplan für den Fall von unberechtigtem Zugriff oder Datenverlust wird derzeit erweitert (Stand 10.08.2018).
Zuständigkeit: windata GmbH & Co.KG, Administration, Geschäftsführung

8. 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 aktuellsten 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. „Richtline für Benutzerkonten, Benutzerrechte und Passwörter" geregelt.
Hersteller: Microsoft
Zuständigkeit: windata GmbH & Co.KG, Administration, 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 & Co.KG, Administration, Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

c. Pseudonymisierung (Produkte)
Eigene (selbstentwickelte) Softwareprogramme wurden angepasst um Pseudonymisierung gem. DSGVO zu gewährleisten
Zuständigkeit: windata GmbH & Co.KG, Entwicklung, Geschäftsführung
Überprüfung: Vor Releasefreigabe durch DSB windata

d. Prozesse zur Wahrung von Betroffenenrechten
gem. interner Richtline und Prozesse; Checklisten; Formulare
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung, Datenschutzbeauftragte Überprüfung: Umgehend nach Durchführung durch DSB windata

Maßnahmen in Planung/Vorbereitung

Maßnahmen zur Pseudonymisierung (gem. Art. 32 Abs. 1 lit. a DSGVO und Art. 25 Abs. 1 DSGVO) personenbezogener Daten und Sicherung von Betroffenenrechten

a. Software-Updates
Aktualisierung der eingesetzten Softwareprogramme zur Verarbeitung von Kun-dendaten, sobald DSGVO-konforme Versionen von den Herstellern bereitgestellt werden
Zuständigkeit: windata GmbH & Co.KG, Administration, Geschäftsführung

9. 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 & Co.KG, Geschäftsführung
Überprüfung: mind. 2 Mal jährlich durch DSB windata

b. Verschiedene Softwareprogramme
Nach Art und Zweck der Daten getrennte Verarbeitung
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung
Überprüfung: mind. 1 Mal jährlich bzw. nach Releasewechsel durch DSB windata

c. Mandantentrennung
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

10. 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 & Co.KG, Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

b. Kompetenz- und Zuständigkeitsregelungen
Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeiter_innen
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung
Überprüfung: mind. 1 Mal jährlich durch DSB windata

c. Kontrolle und Überprüfung
weisungsgebundener Auftragsdurchführung
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung,
Datenschutzbeauftragte Überprüfung: mind. 1 Mal jährlich durch DSB windata

d. Verpflichtung der Mitarbeiter_innen zur Vertraulichkeit
über Anstellungsvertrag und zusätzliche, tätigkeitsbezogene Vertraulichkeitsvereinbarung
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung,
Datenschutzbeauftragte 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-Mail Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung,
Datenschutzbeauftragte Überprüfung: mind. 2 Mal jährlich durch DSB windata

f. Datenschutzbeauftragte
Benennung einer Beauftragten für den Datenschutz (gem. Artikel 37 ff. DSGVO) und einer Stellvertretung
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung

g. Verarbeitungsverzeichnis
Führen eines Verzeichnisses der Verarbeitungstätigkeiten gem. Artikel 30 Abs. 2 DSGVO
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung,
Datenschutzbeauftragte Überprüfung: mind. 1 Mal jährlich durch DSB windata

h. Prozesse zur Einhaltung der DSGVO
Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten und Prozesse zur Weiterleitung von Betroffenenanfragen
→ noch zu erledigen
Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung, Datenschutzbeauftragte

Freigegeben zur Veröffentlichung am 03.09.2018

Michael Rudhart
Geschäftsführer

Lena Balk
Beauftragte für den Datenschutz

windata GmbH & Co.KG
Gegenbaurstraße 4
88239 Wangen im Allgäu
Telefon +49 7522 9770-0
Telefax +49 7522 9770-179
Email info@windata.de

Geschäftsführer:
Josef Baumann, Michael Rudhart

Handelsregister Ulm HRA 720688
Umsatzsteuer-ID DE256165143

Beauftragte für den Datenschutz:
Lena Balk, MA
stv. Beauftragte für den Datenschutz:
Ina Roth

persönlich haftende Gesellschafterin:
windata Verwaltungs GmbH
Gegenbaurstraße 4
88239 Wangen im Allgäu

Geschäftsführer:
Josef Baumann, Michael Rudhart

Handelsregister Ulm HRB 620897