

## Vertrag zur Auftragsverarbeitung

zwischen

-Verantwortlicher – nachstehend „Auftraggeber“ genannt-

und der

windata GmbH & Co. KG, Gegenbaurstraße 4, 88239 Wangen

- Auftragsverarbeiter – nachstehend „Auftragnehmer“ genannt

### 1. Gegenstand und Dauer des Auftrags

#### (1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Dienstleistungsvertrag/ Rahmenvertrag vom \_\_\_\_\_, auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

*(Definition der Aufgaben)*

#### (2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder

Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum

oder

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von Tagen zum gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

## **2. Konkretisierung des Auftragsinhalts**

### **(1) Art und Zweck der vorhergesehenen Verarbeitung von Daten**

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom

oder

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Das angemessene Schutzniveau in

ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);

wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m 47 DSGVO);

wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. C und d DSGVO);

wird hergestellt durch genehmigte Verhaltensregeln (Art.46 Abs. 2 lit. e i.V.m. 40 DSGVO);

wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO).

wird hergestellt durch sonstige Maßnahmen:

(Art. 46 Abs 2 lit. a, Abs. 3 lit. a und b DSGVO)

## **(2) Art der Daten**

Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter:

oder

Gegenstand der Vereinbarung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

Personendatenstamm

Kommunikationsdaten (z.B. Telefon, E-Mail)

Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

Kundenhistorie

Vertragsabrechnungs- und Zahlungsdaten

Planungs- und Steuerungsdaten

Auskunftsangaben (von Dritten, z.B. Auskunftsteien, oder aus öffentlichen Verzeichnissen)

Sonstige:

## **(3) Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:

oder

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Kunden

Interessenten

Abonnenten

Beschäftigte

Lieferanten

Ansprechpartner

Sonstige:

### **3. Technisch-organisatorische Maßnahmen**

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

### **4. Berichtigung, Einschränkung und Löschung von Daten**

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an

den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit nicht vom Leistungsumfang umfasst, sind Löschkonzepte, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

Schriftliche Bestellung eines Datenschutzbeauftragten/einer Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Dessen/Deren Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des/der Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Als Datenschutzbeauftragter/Datenschutzbeauftragte ist beim Auftragnehmer Frau Lena Balk, MA und als Stevertreterin Frau Ina Roth bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Dessen/Deren jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner\_in beim Auftragnehmer wird

Anrede

Name, Vorname

Organisationseinheit

Telefon

E-Mail

benannt.

Der Auftragnehmer hat seinen Sitz außerhalb der Union und benennt folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union

Land

Anrede

Name, Vorname

Organisationseinheit

Telefon

E-Mail

Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem

Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## 6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Eine Unterbeauftragung ist unzulässig

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

**Firma**

**Anschrift**

**Leistung**

**Unterauftragnehmer**

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen einmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

ist nicht gestattet;

bedarf einer ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## **7. Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.



(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren);

eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

## **8. Mitteilung bei Verstößen des Auftragnehmers**

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

## 9. Weisungsbefugnis des Auftraggebers

- (1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien und Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hier- von ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsmäßi- gen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung ge- setzlicher Aufbewahrungspflichten erforderlich sind.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nut- zungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis ste- hen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsmäßigen Datenverarbei- tung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zur Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort und Datum

Ort und Datum

---

*Unterschrift(en) Auftraggeber*

---

*Unterschrift(en) Auftragnehmer*

# 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 vorheriger 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 Zeitabständen 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 unterliegt 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 „Richtlinie 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 „Richtlinie 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 „Richtlinie 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 „Richtlinie 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 einer (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, 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. 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 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

**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 „Richtlinie 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 „Richtlinie 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 „Richtlinie 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 „Richtlinie 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 „Richtlinie 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 „Richtlinie 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, Nadlerstraße 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. „Richtlinie für E-Mail“. Ein- und ausgehende E-Mails werden über ein eigenes, intern betriebenes Mailsystem über das SMTPS-Protokoll mit TLS/SSL-Authentifizierung 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 „Richtlinie 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 „Richtlinie 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 „Richtlinie für Informations- und Kommunikationstechnik (IuK)“  
Überprüfung: mind. 1 Mal jährlich durch DSB windata
- c. **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
- d. **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
- e. **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

## 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 Sorgfaltsgesichtspunkten 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 Einhaltung 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 Geschäftsführung

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 (Feuermelder) 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. „Richtlinie 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 Richtlinie 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 Kundendaten, 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](mailto: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



# DATENSCHUTZERKLÄRUNG

Die windata GmbH & Co.KG, Gegenbaurstraße 4, 88239 Wangen im Allgäu, Deutschland (nachfolgend als „windata“ bezeichnet) ist Anbieter von Softwareprogrammen, Dienstleistungen und Online-Angeboten und die dafür verantwortliche Stelle. Wir nehmen den Schutz Ihrer Daten sehr ernst. Die besondere Beachtung der Privatsphäre bei der Verarbeitung personenbezogener Daten ist uns ein wichtiges Anliegen. Mit dieser Datenschutzerklärung informieren wir sie darüber, welche personenbezogenen Daten wir erheben und speichern sowie über Ihre Rechte im Hinblick auf die Verwendung personenbezogener Daten.

## Personenbezogene Daten

Die Nutzung unseres Online-Angebots ist grundsätzlich ohne Offenlegung der Identität und damit anonym möglich. Wir sind bestrebt, so wenige wie möglich personenbezogene Daten zu erheben.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Darunter fallen Informationen wie Name, Adresse, Postanschrift, Telefonnummer, Telefaxnummer, E-Mail-Adresse, Bankverbindungen. Informationen, die nicht direkt mit Ihrer Identität in Verbindung gebracht werden (statistische Daten wie zum Beispiel favorisierte Internetseiten oder Anzahl der Nutzer einer Site) fallen nicht darunter.

Bei jedem Aufruf unserer Internetseiten erheben, verarbeiten und speichern wir kurzfristig und in anonymer Form serverseitig lediglich Zugriffsdaten wie die IP-Adresse, Datum und Uhrzeit des Aufrufs, die Ursprungs-Internetseite (Referer-URL) und betrachtete Seiten. Diese Zugriffsdaten verwenden wir ausschließlich in anonymer Form, um die Nutzung unseres Online-Angebotes zu ermöglichen und um unser Angebot weiter zu optimieren. Eine Weitergabe dieser Daten an Dritte findet in keinem Falle statt.

## Kinder und Jugendliche

Die Webseiten und Angebote der windata GmbH & Co.KG sind nicht für Personen unter 16 Jahren vorgesehen. Wenn Sie jünger als 16 Jahre sind, dürfen Sie die Webseiten und Angebote nicht nutzen.

## Zweck der Datenerhebung und Speicherung

Soweit überhaupt erforderlich, erheben, speichern und verarbeiten wir personenbezogene Daten ausschließlich nach den geltenden gesetzlichen Bestimmungen und soweit dies zur Erfüllung der vertraglichen Beziehungen zwischen uns und dem Nutzer/der Nutzerin bzw. zur Bereitstellung der angeforderten Angebote notwendig und erforderlich oder zu Abrechnungszwecken erforderlich ist. Eine Nutzung personenbezogener Daten zu Werbezwecken findet nur mit Ihrer ausdrücklich erklärten Einwilligung statt. Eine Weitergabe an Dritte ist ausgeschlossen.

windata erhebt personenbezogene Daten zum Zweck

- a) der Angebotserstellung und/oder
- b) zur Durchführung von Verträgen und/oder
- c) zur Erfüllung von vertraglichen und vorvertraglichen Pflichten und/oder
- d) zur Bereitstellung von Informationen (Updates, Sicherheitshinweise), die sich auf eine vertragsgegenständliche Software oder Dienstleistung beziehen und/oder
- e) zur Erfüllung von Dienstleistungs- und Serviceverpflichtungen die aus Verträgen mit Dritten (z.B. Kreditinstitute, Organisationen, Unternehmen) und/oder Auftragsverarbeitern beruhen und/oder
- f) zur Direktwerbung.

Die Datenerhebung und Datenverarbeitung ist für die Durchführung des Vertrags erforderlich und

beruht auf Artikel 6 Abs. 1 b) und Abs. 1 c) der Datenschutzgrundverordnung (DSGVO).

### Support für Softwareprogramme

Im Falle einer Inanspruchnahme von Dienstleistungen durch einen Vertragspartner/eine Vertragspartnerin zu einem erworbenen bzw. lizenzierten Produkt (Support) ist zur Erfüllung der vertraglichen Leistungen durch windata die Speicherung von Kontaktdaten (personenbezogenen Daten) wie Name, Telefonnummer, E-Mail-Adresse und gegebenenfalls der Sachverhalt der Supportanfrage erforderlich. Die Speicherung erfolgt ausschließlich zur Erfüllung der vertraglichen Leistungen aus dem Kauf-, Lizenz-, Nutzungs- und/oder Servicevertrag. Nach Abschluss einer Supportanfrage – jedoch spätestens nach 30 Kalendertagen – erfolgt eine automatische Löschung der gespeicherten Daten. Erfolgt aufgrund entwicklungs technischer Erfordernisse kein Abschluss der Supportanfrage innerhalb von 30 Kalendertagen, können in Ausnahmefällen die zur Erfüllung der vertraglichen Leistung notwendigen und erbrachten Daten erst nach erfolgreicher Erfüllung gelöscht werden. Diese Verzögerung der Löschung dient ausschließlich dem Kundenservice.

### Kontaktaufnahme

Im Falle einer erwünschten Kontaktaufnahme reichen grundsätzlich die Angabe eines Namens und die Angabe der E-Mail-Adresse und/oder der Telefonnummer aus. Soll Material auf dem Postweg versandt werden, so sind mindestens Name und Anschrift erforderlich.

### Newsletter

Wenn Sie sich für unseren Newsletter anmelden wollen, benötigen wir Ihre E-Mail-Adresse und Ihre ausdrückliche Einwilligung. Die von Ihnen angegebene Adresse wird bei uns erst für Werbezwecke freigeschaltet, wenn Sie den Bestätigungslink in der an die angegebene Adresse gesendeten Check-Mail aktivieren. Eine Abmeldung von unserem Newsletter ist jederzeit mit Wirkung für die Zukunft entweder im Newsletter selbst oder per

formloser E-Mail an [newsletter@windata.de](mailto:newsletter@windata.de) möglich, ohne dass Ihnen hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

### Cookies

Cookies sind kleine Datenpakete mit Konfigurationsinformationen. Diese Dateien speichert der Web-Browser auf dem Computer des Nutzers/der Nutzerin, wenn eine Internetseite geöffnet wird. Um unser Online-Angebot zu nutzen, ist die Einwilligung in die Nutzung von Cookies nicht notwendig, jedoch können dadurch möglicherweise nicht alle Funktionen (wie z.B. Warenkorb, Änderungen von Funktionserweiterungen bei noch nicht vollständig abgeschlossenem Kauf- bzw. Lizenzierungsvorgang) angeboten werden. In den Browsereinstellungen des Nutzers kann das Speichern von Cookies deaktiviert werden. Weitere Hinweise zu der Deaktivierung von Cookies entnehmen Sie bitte Ihrer jeweiligen Browsersoftware.

### Auskunfts- und Löschungsrecht

Sie haben jederzeit das Recht, Auskunft über die von uns erhobenen und gespeicherten Daten sowie bei Unrichtigkeit der Daten deren Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu verlangen. Schreiben Sie uns einfach eine E-Mail an: [datenschutz@windata.de](mailto:datenschutz@windata.de)

Auskunfts-, Löschungs- und Berichtigungswünsche zu Ihren bei uns gespeicherten Daten können Sie jederzeit auch an folgende Adresse senden:

**An die  
Datenschutzbeauftragte  
c/o windata GmbH & Co.KG  
Gegenbaurstraße 4  
88239 Wangen im Allgäu**

Sollten Sie Fragen, Anregungen oder Wünsche zum Thema Datenschutz haben, wenden Sie sich bitte an [datenschutz@windata.de](mailto:datenschutz@windata.de)

Stand: 24. April 2018

**windata GmbH & Co.KG**  
Gegenbaurstraße 4  
88239 Wangen im Allgäu  
Telefon +49 7522 9770-0  
Telefax +49 7522 9770-179  
Email [info@windata.de](mailto:info@windata.de)

Geschäftsführer: Josef Baumann, Michael Rudhart  
Handelsregister Ulm HRA 720688  
Umsatzsteuer-ID DE256165143

persönlich haftende Gesellschafterin:  
windata Verwaltungs GmbH  
Gegenbaurstraße 4  
88239 Wangen im Allgäu  
Geschäftsführer: Josef Baumann, Michael Rudhart  
Handelsregister Ulm HRB 721386

Beauftragte für den Datenschutz: Lena Balk, MA  
stv. Beauftragte für den Datenschutz: Ina Roth  
[datenschutz@windata.de](mailto:datenschutz@windata.de)

Kreissparkasse Ravensburg  
IBAN DE69 6505 0110 0018 3880 99  
BIC SOLADES1RVB

GLS Gemeinschaftsbank eG  
IBAN DE73 4306 0967 7033 4276 00  
BIC GENODEM1GLS

Raiffeisenbank Ravensburg eG  
IBAN DE04 6506 2577 0055 0000 02  
BIC GENODES1RRV