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:

(2) Ort der Datenverarbeitung

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

2.2. Die Übermittlung personenbezogener Daten in ein Drittland oder an internationale Organisationen bedarf der vorherigen Zustimmung des Auftraggebers. Sie wird nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 50 DSGVO erfüllt sind.

2.3 Erfolgt die Übermittlung auf Grundlage von EU-Standardvertragsklauseln, so sichert der Auftragnehmer zu, dass er diese einhalten kann und nicht durch gesetzliche oder andere rechtliche Anforderungen daran gehindert ist. Der Auftragnehmer gibt auf Anfrage Auskunft über die in seinem Land geltenden Gesetze (insbesondere Zugriffsmöglichkeiten durch Behörden des Drittlandes auf die Daten, den Parteien und den betroffenen Personen zustehende Rechtsschutzmöglichkeiten, Rechtsprechung und Behördenpraxis im Drittland mit Bezug zum Datenschutzniveau und zum Rechtssystem insgesamt) und weist nach, dass sie den durch die EU-Standardvertragsklauseln gewährten Schutz nicht untergraben.

2.4 Sofern der Schutz der im Auftrag verarbeiteten personenbezogenen Daten durch Gesetze oder eine sonstige Praxis im Zielland beeinträchtigt wird, hat der Auftragnehmer zusätzliche Maßnahmen (z. B. Verschlüsselung, Anonymisierung, Pseudonymisierung, Trustee-Lösung etc.) umzusetzen, um einen wirksamen Schutz herzustellen. Der Auftragnehmer gibt auf Anfrage Auskunft über die ergriffenen zusätzlichen Maßnahmen.

2.5 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er nicht mehr in der Lage ist, die EU-Standardvertragsklauseln einzuhalten; in diesem Fall darf der Auftraggeber die Datenübermittlung aussetzen und den Hauptvertrag mit dem Auftragnehmer kündigen. Der Auftragnehmer hat betroffene Personen verschuldens-unabhängig von allen Schäden freizustellen, die durch den Zugriff von Stellen seines Staates bzw. am Ort der Datenverarbeitung außerhalb der EU auf die Daten der betroffenen Personen entstehen.

(3) 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. Auskunfteien, oder aus öffentlichen Verzeichnissen)

☐ Sonstige:

(4) Kategorien betroffener Personen

○ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungs-vereinbarung konkret beschrieben unter:

oder

- [x] Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
  - [ ] Kunden
  - [ ] Interessenten
  - [ ] Abonnenten
  - [ ] Beschäftigte
  - [ ] Zahlungspflichtige/Zahlungsempfänger
  - [ ] 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 Vergessen-werden, 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 externer Datenschutzbeauftragter ist beim Auftragnehmer PRW Consulting GmbH, Leonrodstrasse 54, 80636 München, Herr Marcel Erntges, Tel.: +49 (0)89 / 2109 77 - 70, E-Mail: marcel.erntges@prw-consulting.de bestellt. Stellvertreterin ist windata GmbH & Co KG, Gegenbaurstr. 4, 88239 Wangen, Tel.: +49 (0) 7522 / 9770-0, E-Mail: datenschutz@windata.de. 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 Herr

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 Herr

Name, Vorname

Organisationseinheit

Telefon

E-Mail

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

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

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

c) 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.

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

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seine Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

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

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz Aufsichtsbehörde.

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 Unterauftragnehmer	Anschrift	Leistung

☐ 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 Unterauftrag - nehmer 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 Unter-auftragnehmer 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 über-zeugen.

(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, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

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

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

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. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsmäßigen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher 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 Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, 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 Datenverarbeitung 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) - 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
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 Videos 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 „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 einer (hardwarebasierten) Sophos Red-Box. Die Ausgabe der Red-Box wird durch den Administrator verwaltet, kontrolliert und protokolliert
Hersteller: SOPHOS
Model: RED/ SOPHOS ConnectClient
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, die Geschäftsführung. Ersatzschlüssel ist nur bestimmten ausgewählten Personenkreis zugänglich.
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: Microsoft
- **iii.** Route/Gateway (IDS)
  Hersteller: SOPHOS
- **iv.** Serversysteme (Anti-Viren)
  Hersteller: Microsoft
- **v.** 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 „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 die betriebliche 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 300 Mbit SDSL Glasfaserverkabelung hergestellt bzw. 1000/50 Mbit/s Vodafone
Betreiber: Telekommunikation Lindau (B) GmbH, Auenstraße 12, 88131 Lindau
Zertifikate: TÜViT Level3
Zuständigkeit: Telekommunikation Lindau (B) GmbH, Administration
Fallback: Koaxialverbindung, Vodafone
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-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 „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 im Datensystem gem. interner „Richtline für Informations- und Kommunikationstechnik (IuK)" Überprüfung: mind. 1-mal jährlich durch DSB windata

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

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

d. 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 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 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:. 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 & Co.KG, 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. 6. a.
Zuständigkeit: windata GmbH & Co.KG, Datenschutzbeauftragte und Geschäftsführung
Überprüfung: min. 1-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 APC-SRT5KRMXLI
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, Richthofenstr. 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 (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 & Co.KG, Administration, Geschäftsführung
Überprüfung: mind. 1-mal jährlich durch DSB windata

f. Notfallplan
Ein Notfallplan für interne IT-Systeme ist vorhanden.
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 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. „Richtline für Benutzerkonten, Benutzerrechte und Passwörter" geregelt.
Hersteller: Microsoft
Zuständigkeit: windata GmbH & Co.KG, 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 & Co.KG, Entwicklung, 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 Release Freigabe 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 Kundendaten, sobald DSGVO-konforme Versionen von den Herstellern bereitgestellt werden
Zuständigkeit: windata GmbH & Co.KG, Entwicklung, 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
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,
Überprüfung: mind. 1-mal jährlich durch DSB windata

d. Verpflichtung der Mitarbeiter zur Vertraulichkeit
über Anstellungsvertrag und zusätzliche, tätigkeitsbezogene Vertraulichkeitsvereinbarung
Zuständigkeit: windata GmbH & Co.KG, 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- Mail Zuständigkeit: windata GmbH & Co.KG, Geschäftsführung,
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
Überprüfung: mind. 1-mal jährlich durch DSB windata

Freigegeben zur Veröffentlichung April 2023

windata GmbH & Co. KG
Gegenbaurstraße 4
88239 Wangen im Allgäu

Telefon +4 97522 9770-0
Telefax +4 97522 9770-179

Email info@windata.de

www.windata.de
www.windata.de/impressum

Beauftragte für den Datenschutz:
PRW Consulting GmbH Marcel Erntges LL.B ., MA stv.

Beauftragte für den Datenschutz:
datenschutz@windata.de