Vereinbarung zur Auftragsdatenverarbeitung

Zwischen
xxxxxx
- nachstehend Auftraggeber genannt -

Und der WorNet AG, Bürgermeister-Graf-Ring 28, D-82538 Geretsried
- nachstehend Auftragnehmer genannt -

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Nutzungsvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Nutzungsvertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Nutzungsvertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

Der Kreis der betroffenen Personen sowie die Art der personenbezogenen Daten, die von der Auftragsverarbeitung betroffen sind, ist in Anlage 2 „Auftragsdetails“ beschrieben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmenseiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. (Anmerkung: Im Vertrag können die Parteien hierzu eine Vergütungsregelung treffen).

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmendes Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

§9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion

Anlagen:

- 1: Technisch Organisatorische Maßnahmen
- 2: Auftragsdetails

Anlage 2: Auftragsdetails

(Zutreffendes bitte ankreuzen)

A2.1. Kategorien von betroffenen Personen

Die Datenverarbeitung betrifft folgende Kategorien von natürlichen Personen:

- ☒ Beschäftigte und ehemalige Beschäftigte
- ☐ Webseitenbesucher
- ☐ Kunden, Klienten, Patienten
- ☒ Kommunikationspartner (E-Mail)
- ☐ Lieferanten
- ☐ Ansprechpartner
- ☐ Interessenten
- ☐ Handelspartner
- ☒ Abonnenten
- ☐ Weitere:

A2.2. Arten der personenbezogenen Daten

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien:

Personenstammdaten

- ☒ Name/Vorname
- ☐ User-ID/ Benutzererkennung
- ☒ Kommunikationsdaten (Telefonnummer, Email, etc.)
- ☒ Personenbeziehbare Daten wie z.B. IP Adresse, Rechnernummer, etc.
- ☒ Zugriffsberechtigungen für Systeme
- ☐ Geburtsdatum
- ☐ Zeitwirtschaftsdaten
- ☐ Kostenstelle/Abteilungskürzel
- ☐ Abrechnungsdaten bzw. Gehaltsdaten, Bankdaten, etc.
- ☐ Karriere- und Potentialdaten
- ☐ Daten zu Dienstreisen
- ☐ Daten zu Veranstaltungen
- ☐ Gesundheitsdaten
- ☐ Weitere:

Telekommunikationsdaten

- ☒ Nutzungsdaten aus Telemediendiensten und Telekommunikationsdiensten
- ☐ Weitere:

Organisationsdaten

- ☒ Struktur der Abteilungen sowie deren Ansprechpartner
- ☒ Organisationsdiagramme sowie deren Ansprechpartner
- ☐ Weitere:

Kundendaten

- ☒ Kundenhistorie mit Personenbezug
- ☒ Ansprechpartner
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Weitere:

Sonstiges

- ☒ Protokollierungsdaten mit Personenbezug
- ☐ Weitere

A2.3. Weisungen zum Umgang mit personenbezogenen Daten

Der Auftragnehmer ist an die Weisungen des Auftraggebers gebunden und verfolgt mit der Datenverarbeitung keinerlei eigene Interessen. Die Weisungen, die sich aus dem Auftrag ergeben und Auswirkungen auf die Verarbeitung personenbezogener Daten haben sind vom Auftraggeber zu dokumentieren (Art. 28 Abs 3. DSGVO).

Serverbetrieb

☐ Betrieb von Webservern (unten spezifiziert)
☐ Betrieb von Datenbankservern (unten spezifiziert)
☒ Betrieb von E-Mailservern
☐ Wartung von Betriebssystemen
☐ Datenstandort: WorNet-Serverfarm (München, Pettenkoferstr. 22a)
☐ Datenstandort: WorNet-Serverfarm (München, Weimarerstr. 22)
☐ Backupstandort: WorNet-Serverfarm (München, Göthestr. 10)
☐ Backupstandort: WorNet-Serverfarm (München, Weimarerstr. 22)
☐ Sonstige Datenspeicherorte: nein
☐ Übermittlung von Daten zur Verarbeitung an Dritte: nein
☒ Löschung von DV-Protokollen nach 28 Tagen
☐ Weitere / Spezifikation:

Telekommunikationsleistungen

☒ Übermittlung von E-Mails
☐ Betrieb von E-Mail-Postfächern
☐ Betrieb von Telefonie-/Video-/Chat-Systemen
☐ Betrieb von Datenaustauschplattformen
☐ Betrieb von VPNs (Virtuelle Private Netzwerke)
☐ Betrieb von Webseitenanalyse (Matomo)
☐ Weitere:

Datensicherung / Verfügbarkeit

☒ Redundante Speicherung von Daten während der Verarbeitung (alle SLAs)
☒ Tägliche Datensicherung an Backup-Standort (SLA Gold)
☒ Wöchentliche Datensicherung am gleichen Standort (SLA Silber)
☐ Weitere:

Sonstiges

Datum: 28. März 2022

Unternehmen: WorNet AG, Bürgermeister-Graf-Ring 28, 82538 Geretsried

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

a. Zutrittskontrolle

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

☒ Ausreichend abgesicherte Zugänge
(Türen, Türschlösser, Lichtschächte, Lüftungsöffnungen, Fenster, Verglasungsart, Rollos gegen Hochschieben gesichert, Feuerleiter, Feuertreppe, elektrische Türöffner)

☒ Heimarbeiten/Telearbeiten nur per VPN

☒ Überwachungseinrichtung (Alarmanlage, Videoüberwachung)

☒ Schriftliche Festlegungen zur Zugangsberechtigung, Ausweisregelungen

Rechenzentrum Pettenkofer-/Goethestr. (Betreiber WorNet AG):

☒ Zutrittskontrollsystem mit zwei Stufen (Gebäude (Schlüssel), Raum (PIN))

☒ Lage des Rechenzentrums/Serverräume im Gebäude: Hochparterre (Serverraum) und Keller (Backupstandort)

☒ Protokollierung von Aufenthalten im Sicherheitsbereich

Rechenzentrum Weimarerstr. (Betreiber M-Net GmbH):

☒ Zertifizierung nach ISO/IEC 27001 des Rechenzentrumsdienstleisters (M-Net)

☒ Trennung von Bearbeitungs- und Publikumszonen, Besucherregelungen, Besucherbuch

☒ Zutrittskontrollsystem mit vier Stufen (Gebäude (Chip+PIN), Flur (Fingerabdruck), Raum (Chip) und Schrank (Chip))

☒ Lage des Rechenzentrums/Serverräume im Gebäude: Hochparterre, Serverräume als separate Zellen (Zutritt, Brandschutz)

☒ Protokollierung von Aufenthalten im Sicherheitsbereich (durch Rechenzentrumsbetreiber)

Zutritt haben:

☒ nur zuständige MitarbeiterInnen (abgestufte Zutrittsregelungen)

b. Zugangskontrolle

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

☒ geeignete Passwortverfahren (Mindestlänge acht Stellen)

☒ regelmäßiger Wechsel des Passworts alle 12 Monate)

☒ automatische Sperrung der Bildschirme mit Passwortschutz bei Pausen

☒ jede/r Mitarbeiter/in erhält einen eigenen Benutzerstammsatz

☒ Festplatten der Laptops und PCs sind verschlüsselt

c. 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 (Zugriffskontrolle),

☒ Berechtigungskonzept (sowohl für Anwender, wie auch für Administratoren)

☒ differenzierte Berechtigungen für Auswertungen, Kenntnisnahme, Veränderung, Löschung

☒ Schutz gegen unberechtigte interne und externe Zugriffe vorhanden (Verschlüsselung, Firewall)

☒ Überwachung und Protokollierung, sowie Auswertung der Zugriffe bzw. Zugriffsversuche

☒ Protokoll-Aufbewahrungszeit: 4 Wochen

☒ Datenträgerverwaltung, Nachweis über Eingang, Nutzung, Ausgang/Vernichtung

☒ äußerliche Kennzeichnung der Datenträger

☒ Verbot des Einsatzes privater Datenträger

☒ fachgemäße Entsorgung/Vernichtung von Fehldrucken, veralteten Datenträgern etc. sichergestellt

d. Trennungskontrolle

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

☒ Mandantenfähigkeit – Software-/Hardwareseitig

☒ getrennte DV-Systeme für unterschiedliche Verarbeitungszwecke vorhanden

☒ Datenbanken: Trennung über Zugriffsregelung

☒ Trennung von Administration, Test- und Produktivumgebung

e. Pseudonymisierung

Eine Verarbeitung personenbezogener Daten, die sich pseudonymisieren ließen findet nicht statt.

2. INTEGRITÄT (Art. 32 Abs. 1 lit. b DS-GVO)

a. 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle).

Die Weitergabe von Daten erfolgt ausschließlich datenträgerlos über verschlüsselte und passwortgesicherte Netzverbindungen

b. Eingabekontrolle

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

- ☒ Protokollierung je nach System (Aufbewahrungsdauer: 4 Wochen)
- ☒ Dokumentation der Eingabeverfahren (Dienstanweisung)

3. VERFÜGBARKEIT und BELASTBARKEIT (Art. 32 Abs. 1 lit. b DS-GVO)

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle) und rasch wiederhergestellt werden können.

- ☒ Brandschutzeinrichtungen (Feuerlöschanlage (nur Weimarerstr.), Rauch- und Brandmelder)
- ☒ Unterbrechungsfreie Stromversorgung (USV), Notstromversorgung
- ☒ Datensicherung an 2. Standort (Göthestraße, nur bei SLA Gold und Platin)
- ☒ Dokumentation und regelmäßige Tests des Back-Up Verfahrens
- ☒ Festplatten gespiegelt: RAID 6, RAID10 oder VMware vSAN mit 2 Replicas
- ☒ Virenschutz/Firewall mit automatischer Aktualisierung und Monitoring
- ☒ Ausweichrechenzentrum (Pettenkoferstraße)

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a. Datenschutz-Management

- ☒ Zertifizierung nach ISO/IEC 27001
- ☒ Dokumentation von Requests, Changes und Incidents per Ticketsystem
- ☒ Datenschutzdokumentation
- ☒ Schriftliche Arbeitsanweisungen

☒ Keine Verträge mit Drittländern

b. Incident-Response-Management

Es ist zu gewährleisten, dass eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt und voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt, fristgemäß innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde gemeldet werden kann.

☒ interne Richtlinie für den Fall einer Datenpanne, insbesondere Definition von Datenpannen, Festlegung von Data-Breach-Notification-Verantwortlichen und weiteren Ansprechpartnern, Schaffung eines Krisenteams und Unterrichtung sämtlicher Mitarbeiter

☒ alle gemeldeten oder nicht gemeldeten aber bekannten Verletzungen werden dokumentiert einschließlich aller mit dieser, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen im Zusammenhang stehenden Fakten

c. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Es ist zu gewährleisten, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden (Datenschutz durch Voreinstellungen).

☒ Bestehen Voreinstellungen, die gewährleisten, die Menge der verarbeiteten Daten so weit wie möglich reduziert wird?

☒ Bestehen Voreinstellungen, die den Umfang der Datenverarbeitung auf das erforderliche Maß beschränken?

☒ Vorgegebene Speicherfristen: 4 Wochen

d. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).

☒ Für die Verarbeitung personenbezogener Daten werden keine Unterauftragnehmer eingesetzt.

☒ Die Verarbeitung personenbezogener Daten erfolgt nur im Umfang und auf Weisung des Auftraggebers.

☒ Änderungen an Verfahren erfolgen nur nach schriftlicher Bestätigung durch den Auftraggeber

☒ Der Auftraggeber wird über Programmfehler oder Abbrüche informiert.

Solange bei der WorNet AG nicht mehr als 19 Personen ständig mit der Verarbeitung personenbezogener Daten beauftragt sind ist der Vorstand Christian Eich Ansprechpartner für alle Fragen des Datenschutzes.

Geretsried, den 28. März 2022	**Geretsried, den 28. März 2022**
Christian Eich	**Hannes Wilhelm**
Vorstand	**IT-Leiter**