Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

– Vorlage wildweiss GmbH (Stand: 2025-12-18) –

zwischen

_____
[Name/Firma Verantwortlicher]

_____
[Straße, Hausnummer]

_____
[PLZ, Ort]

– nachfolgend „Verantwortlicher“ –

und

wildweiss GmbH
Kiefernsteig 2
90607 Rückersdorf

– nachfolgend „Auftragsverarbeiter“ –

Verantwortlicher und Auftragsverarbeiter werden gemeinsam auch „Parteien“ genannt.

Präambel

Die Parteien haben einen Vertrag über Leistungen im Bereich Personalgewinnung (nachfolgend „Hauptvertrag“) geschlossen oder beabsichtigen, einen solchen zu schließen. Soweit der Auftragsverarbeiter dabei personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, gilt dieser Auftragsverarbeitungsvertrag („AVV“).

§ 1 Gegenstand, Geltungsbereich und Begriffe

1. Dieser AVV regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen gemäß Art. 28 DSGVO.

2. Dieser AVV ist Bestandteil des Hauptvertrags. Im Falle von Widersprüchen gehen die Regelungen dieses AVV für die Verarbeitung personenbezogener Daten vor.

3. Begriffe werden entsprechend Art. 4 DSGVO verwendet.

§ 2 Beschreibung der Verarbeitung

1. Gegenstand, Art, Zweck und Dauer der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen ergeben sich aus Anlage 1 („Verarbeitungsspezifikationen“).

2. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zur Erbringung der Leistungen aus dem Hauptvertrag und nach dokumentierten Weisungen des Verantwortlichen.

§ 3 Weisungen des Verantwortlichen

1. Weisungen werden durch den Verantwortlichen mindestens in Textform (z. B. E-Mail) erteilt. Standardisierte Abläufe, die im Hauptvertrag, in diesem AVV oder in Anlage 1 beschrieben sind, gelten als dokumentierte Weisungen.

2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Der Auftragsverarbeiter ist berechtigt, die Ausführung einer offensichtlich rechtswidrigen Weisung bis zur Klärung auszusetzen.

3. Soweit Weisungen oder Unterstützungsleistungen einen Mehraufwand verursachen, der nicht vom Hauptvertrag umfasst ist (z. B. besondere Exporte, Sonderauswertungen), kann der Auftragsverarbeiter hierfür eine angemessene Vergütung verlangen.

4. Der Verantwortliche stellt sicher, dass nur weisungsberechtigte Personen Weisungen erteilen. Eine namentliche Benennung ist nicht erforderlich; auf Anfrage teilt der Verantwortliche dem Auftragsverarbeiter die weisungsberechtigten Kontaktstellen mit.

§ 4 Pflichten und Rechte des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich (insb. Rechtsgrundlagen, Informationspflichten, Einwilligungen/Berechtigte Interessen, Löschkonzept und Aufbewahrungsfristen, Beachtung von § 26 BDSG und einschlägigen arbeitsrechtlichen Vorgaben).

2. Der Verantwortliche ist dafür verantwortlich, Bewerberinnen und Bewerber über die Verarbeitung – einschließlich der Einbindung des Auftragsverarbeiters, der genutzten Kommunikationskanäle (z. B. E-Mail/WhatsApp) und relevanter Empfänger – in geeigneter Weise zu informieren.

3. Der Verantwortliche entscheidet über die Verwendung/Übernahme von Bewerberdaten in eigene Systeme und ist für dortige weitere Verarbeitung und Aufbewahrung verantwortlich.

4. Der Verantwortliche ist verpflichtet, dem Auftragsverarbeiter nur solche personenbezogenen Daten zur Verfügung zu stellen, deren Verarbeitung rechtmäßig ist und die für den Zweck erforderlich sind (Datenminimierung).

§ 5 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, soweit keine gesetzliche Verarbeitungspflicht besteht.

2. Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind und nur im erforderlichen Umfang Zugriff erhalten (Need-to-know).

3. Der Auftragsverarbeiter ergreift die in Anlage 3 beschriebenen technischen und organisatorischen Maßnahmen („TOMs“) gemäß Art. 32 DSGVO.

4. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung bei der Erfüllung von Betroffenenrechten sowie bei Datenschutz-Folgenabschätzungen und Konsultationen (Art. 35, 36 DSGVO) nach Maßgabe von § 9.

5. Der Auftragsverarbeiter führt ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO, soweit gesetzlich erforderlich.

§ 6 Unterauftragsverarbeiter

1. Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt.

2. Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 14 Kalendertage vor jeder beabsichtigten Änderung der Unterauftragsverarbeiterliste (Hinzufügen oder Ersetzen) in Textform. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem Grund (insb. Datenschutzrisiken) widersprechen.

3. Widerspricht der Verantwortliche, werden die Parteien eine zumutbare Lösung anstreben (z. B. alternative technische Umsetzung). Ist dies nicht möglich, kann der Verantwortliche den vom Wechsel betroffenen Teil der Leistungen mit einer angemessenen Frist kündigen.

4. Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem im Wesentlichen dieselben Datenschutzpflichten auferlegt wie dieser AVV. Der

Auftragsverarbeiter bleibt für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.

5. Auf Verlangen stellt der Auftragsverarbeiter dem Verantwortlichen Kopien einschlägiger Unterauftragsverarbeitungsverträge in angemessener Weise zur Verfügung; Geschäftsgeheimnisse dürfen geschwärzt werden.

6. Klarstellung: Der Verantwortliche muss mit den vom Auftragsverarbeiter eingesetzten Unterauftragsverarbeitern grundsätzlich keine eigenen AVV abschließen; die vertragliche Einbindung erfolgt über den Auftragsverarbeiter gemäß Art. 28 Abs. 4 DSGVO.

§ 7 Verarbeitung in Drittländern / internationale Übermittlungen

1. Eine Verarbeitung/Übermittlung personenbezogener Daten in Länder außerhalb der EU/des EWR („Drittländer“) erfolgt nur, sofern die Voraussetzungen des Kapitels V DSGVO erfüllt sind (insb. Angemessenheitsbeschluss oder geeignete Garantien wie EU-Standardvertragsklauseln) und nur im Rahmen der beauftragten Leistungen.

2. Soweit Unterauftragsverarbeiter Drittländer einbinden, stellt der Auftragsverarbeiter geeignete Garantien sicher und informiert den Verantwortlichen auf Anfrage über die wesentlichen Schutzmechanismen.

§ 8 Technische und organisatorische Maßnahmen (TOMs)

1. Die TOMs ergeben sich aus Anlage 3.

2. Der Auftragsverarbeiter darf die TOMs unter Berücksichtigung des Standes der Technik weiterentwickeln, sofern das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 9 Unterstützung, Betroffenenanfragen und behördliche Anfragen

1. Der Auftragsverarbeiter beantwortet Anfragen betroffener Personen nicht selbst, es sei denn, er ist hierzu vom Verantwortlichen dokumentiert ermächtigt.

2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Betroffenenanfragen oder behördliche Anfragen, die er in Bezug auf die Auftragsverarbeitung erhält.

3. Soweit Unterstützungshandlungen einen Mehraufwand verursachen, der nicht vom Hauptvertrag umfasst ist (z. B. umfangreiche Auskünfte/Exporte), kann der Auftragsverarbeiter hierfür eine angemessene Vergütung verlangen.

§ 10 Meldung von Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnisnahme, über Verletzungen des Schutzes personenbezogener Daten, die die Auftragsverarbeitung betreffen.

2. Die Meldung enthält – soweit verfügbar – mindestens: Art der Verletzung, betroffene Datenkategorien, ungefähre Anzahl betroffener Personen/Datensätze, mögliche Folgen, ergriffene/empfohlene Maßnahmen sowie eine Kontaktstelle.

3. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

§ 11 Speicher- und Löschfristen während der Vertragslaufzeit

1. Der Verantwortliche weist den Auftragsverarbeiter an, Bewerberdaten im Rahmen der beauftragten Recruiting-Kampagne zu verarbeiten. Der Auftragsverarbeiter löscht die im Auftrag verarbeiteten Bewerberdaten spätestens nach Ablauf von 6 Monaten nach dem Ende der jeweiligen Kampagne, sofern der Verantwortliche keine abweichende Weisung in Textform (z. B. E-Mail) erteilt.

2. Eine frühere Löschung ist jederzeit auf Weisung des Verantwortlichen möglich.

3. Soweit Bewerberdaten in Sicherungskopien/Backups enthalten sind, werden diese im Rahmen der regulären Sicherungszyklen überschrieben bzw. gelöscht und bis dahin gesperrt und nicht produktiv genutzt.

4. Für optionale telefonische Erstgespräche (Anlage 1) können – sofern beauftragt und technisch aktiviert – Gesprächsaufzeichnungen in Close zeitlich begrenzt gespeichert werden (derzeit: 7 Tage). Gesprächstranskripte/Notizen werden nach Maßgabe der Ziff. 1 gelöscht, sofern der Verantwortliche keine abweichende Weisung erteilt. Gesprächsaufzeichnungen und KI-Funktionen werden nur genutzt, wenn dies Bestandteil der beauftragten Leistung ist.

§ 12 Löschung und Rückgabe nach Beendigung

1. Nach Beendigung der Auftragsverarbeitung löscht der Auftragsverarbeiter personenbezogene Daten oder gibt sie nach Wahl des Verantwortlichen zurück, sofern keine gesetzliche Aufbewahrungspflicht besteht.

2. Der Verantwortliche teilt dem Auftragsverarbeiter seine Wahl innerhalb von 30 Kalendertagen nach Vertragsende in Textform mit. Erfolgt keine Mitteilung, ist der Auftragsverarbeiter berechtigt, die Daten zu löschen.

3. Daten in Sicherungskopien (Backups) werden im Rahmen der regulären Backup-Zyklen überschrieben bzw. gelöscht; bis dahin werden sie gesperrt und nicht produktiv genutzt.

4. Auf Wunsch stellt der Auftragsverarbeiter eine Löschbestätigung in Textform aus.

§ 13 Kontrollen und Audits

1. Der Verantwortliche ist berechtigt, die Einhaltung dieses AVV zu kontrollieren. Der Auftragsverarbeiter stellt hierfür in angemessener Weise Informationen (z. B. TOM-Übersicht, Subunternehmerliste) zur Verfügung.

2. Audits sollen grundsätzlich als Dokumenten-/Remote-Audit erfolgen. Vor-Ort-Audits sind nur zulässig, soweit sie erforderlich sind und ein Remote-Audit nicht ausreicht.

3. Audits sind mindestens 14 Kalendertage vorher anzukündigen, außer bei konkreten Anhaltspunkten für eine Nichteinhaltung oder nach einem Sicherheitsvorfall.

4. Audits dürfen den Geschäftsbetrieb nicht unangemessen beeinträchtigen und sind auf einmal pro Kalenderjahr begrenzt, soweit kein Anlass besteht.

5. Die Kosten des Audits trägt der Verantwortliche. Ergibt ein Audit wesentliche, vom Auftragsverarbeiter zu vertretende Verstöße, trägt der Auftragsverarbeiter die angemessenen Kosten der Nachbesserung; weitergehende Kostenregelungen bleiben dem Hauptvertrag vorbehalten.

6. Der Verantwortliche stellt sicher, dass beauftragte Prüfer zur Vertraulichkeit verpflichtet sind.

§ 14 Haftung und Freistellung (Innenverhältnis)

1. Die Haftung der Parteien richtet sich im Außenverhältnis nach Art. 82 DSGVO und den gesetzlichen Bestimmungen.

2. Im Innenverhältnis haften die Parteien einander entsprechend dem Anteil an der Verantwortung für den Schaden. Der Verantwortliche stellt den Auftragsverarbeiter von Ansprüchen Dritter frei, soweit diese auf Weisungen des Verantwortlichen, fehlender/fehlerhafter Rechtsgrundlage, unzureichenden Informationen an Betroffene oder sonstigen Pflichtverletzungen aus dem Verantwortungsbereich des Verantwortlichen beruhen.

3. Soweit rechtlich zulässig, ist die vertragliche Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen für leicht fahrlässige Pflichtverletzungen auf den vertragstypischen, vorhersehbaren Schaden begrenzt. Die Haftungshöchstsumme beträgt 50.000 EUR je Kalenderjahr oder 150 % der im letzten Vertragsjahr gezahlten Nettovergütung aus dem Hauptvertrag (je nachdem, welcher Betrag höher ist).

4. Unberührt bleiben Haftung bei Vorsatz und grober Fahrlässigkeit, bei Verletzung von Leben, Körper oder Gesundheit, nach dem Produkthaftungsgesetz sowie für ausdrücklich übernommene Garantien.

§ 15 Datenschutzkontakt / Datenschutzbeauftragter

1. Der Auftragsverarbeiter hat derzeit keinen Datenschutzbeauftragten bestellt. Eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht nach derzeitigem Stand

nicht. Etwaige gesetzliche Bestellpflichten, insbesondere nach Art. 37 DSGVO i. V. m. § 38 BDSG, bleiben unberührt.

2. Datenschutzkontaktstelle des Auftragsverarbeiters: datenschutz@wildweiss.com. Änderungen teilt der Auftragsverarbeiter in Textform mit.

§ 16 Schlussbestimmungen

1. Änderungen und Nebenabreden bedürfen der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist.

2. Es gilt deutsches Recht. Gerichtsstand für Streitigkeiten aus diesem AVV ist – soweit gesetzlich zulässig – der Sitz des Auftragsverarbeiters.

3. Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Unterschriften

Für den Verantwortlichen	Für den Auftragsverarbeiter (wildweiss GmbH)
_____ Ort, Datum	Rückersdorf, 18.12.2025 _____ Ort, Datum
_____ Name, Unterschrift	Jonathan Albert _____ Name, Unterschrift

Anlage 1 – Verarbeitungsspezifikationen (Art. 28 Abs. 3 DSGVO)

A. Gegenstand und Zwecke der Verarbeitung

• Planung, Umsetzung und Betrieb von Recruiting-Kampagnen (u. a. auf Meta-Plattformen) und Bewerber-Erfassungsstrecken („Kurzbewerbung“) im Auftrag des Verantwortlichen.
• Entgegennahme, Speicherung und strukturierte Aufbereitung von Bewerberdaten zur Weiterleitung an den Verantwortlichen.
• Optionaler Lebenslauf-Upload (Dateispeicherung über Hetzner Online GmbH).
• Standardisierte, automatisierte Bewerberkommunikation (E-Mail über Perspective; WhatsApp-Nachrichten über WhatsApp Business Solution/Cloud API, ausgelöst über Perspective; Versand nur, soweit Bewerber WhatsApp nutzen).
• Optional (nur bei ausdrücklicher Beauftragung): Durchführung telefonischer Erstgespräche zur Verifizierung/Ergänzung der Angaben; Verarbeitung in Close (CRM/VoIP).

B. Kategorien betroffener Personen

• Bewerberinnen und Bewerber
• ggf. Referenzen/Ansprechpersonen, soweit vom Bewerber bereitgestellt

C. Kategorien personenbezogener Daten

• Stammdaten/Kontaktdaten (Name, Telefonnummer, E-Mail, ggf. Wohnort/PLZ, Erreichbarkeitszeiten)
• Bewerbungs-/Karrieredaten (z. B. Qualifikationen, Berufserfahrung, Ausbildungsdaten, Motivation/Freitext – soweit vom Verantwortlichen vorgegeben)
• Upload-Daten (Lebenslauf/Dateianhänge, soweit aktiviert)
• Kommunikationsdaten (Inhalte/Metadaten von E-Mails und WhatsApp-Nachrichten; Gesprächsnotizen bei Erstgesprächen)
• Optional bei Erstgesprächen: Gesprächsaufzeichnungen (Retention derzeit 7 Tage) und Transkripte/Notizen, sofern technisch aktiviert und beauftragt
Hinweis: Bewerbungsunterlagen können besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO enthalten (z. B. Gesundheitsangaben), ohne dass der Verantwortliche oder der Auftragsverarbeiter diese gezielt erhebt.

D. Art der Verarbeitung

• Erheben (Formulareingaben, Uploads)
• Speichern/Strukturieren
• Übermitteln an den Verantwortlichen (z. B. Bereitstellung in Perspective, Benachrichtigungen, Export)
• Kommunikation (E-Mail/WhatsApp)
• (optional) Dokumentation von Gesprächsergebnissen, ggf. Aufzeichnung/Transkription

E. Besonderheiten / Datenminimierung

• Der Auftragsverarbeiter trifft keine eigenen Einstellungs-/Absageentscheidungen.
• Eine automatisierte Bewertung/Scoring findet nicht statt. Es kann vorkommen, dass ein Bewerbungsprozess vor Erhebung personenbezogener Daten endet, wenn Grundvoraussetzungen nicht erfüllt sind (z. B. fehlender Ausbildungsabschluss).

F. Ort der Verarbeitung

• Grundsätzlich EU/EWR.
• Drittländer können über Unterauftragsverarbeiter oder Plattformanbieter eingebunden sein (siehe Anlage 2 und § 7).

G. Dauer der Verarbeitung / Löschkonzept

• Für jede Recruiting-Kampagne bis zum Kampagnenende.
• Standardweisung zur Löschung: spätestens 6 Monate nach Kampagnenende (§ 11), sofern keine abweichende Weisung in Textform erteilt wird.
• Bei optionalen Erstgesprächen: Gesprächsaufzeichnungen in Close werden derzeit nach 7 Tagen gelöscht; Transkripte/Notizen werden nach § 11 gelöscht, sofern keine abweichende Weisung erteilt wird.

Anlage 2 – Unterauftragsverarbeiter (Stand: Vertragsabschluss)

Unterauftragsverarbeiter können als „bedingt“ gekennzeichnet sein (Einsatz nur, wenn die entsprechende Leistung beauftragt/aktiviert wird).

Unterauftragsverarbeiter	Sitz/Land	Leistung	Datenkategorien	Drittlandbezug	Status
Perspective Software GmbH	Deutschland	Recruiting-Funnel/„Kurzbewerbung“, Automationen, Benachrichtigungen, E-Mail-Versand, Speicherung von WhatsApp-Inhalten	Bewerberdaten inkl. Kommunikationsdaten	möglich (Sub-Subprozessoren; Transfermechanismen gem. DPA)	aktiv
Hetzner Online GmbH	Deutschland	Hosting & Dateispeicherung für Lebenslauf-Uploads; systemseitiger E-Mail-Versand (z. B. Link zum Upload)	Upload-Dateien (Lebenslauf), Links/Metadaten	nein	aktiv
Elastic Inc., dba Close (optional)	USA	CRM/VoIP für telefonische Erstgespräche, Call-Logging; optional Aufzeichnung/Transkription (falls beauftragt)	Kontakt-/Bewerberdaten (Teilmengen), Gesprächsnotizen; ggf. Aufzeichnungen/Transkripte	ja (SCC gem. DPA)	bedingt
JOIN Solutions GmbH (JOIN.com) (optional)	Deutschland	Ausspielung/Verwaltung von Stellenanzeigen (falls beauftragt)	Stellenanzeigen-/Bewerberdaten (je nach Setup)	nein (nach Kenntnisstand)	bedingt

Transparenzhinweis zu Plattform-/Kommunikationsanbietern (keine Unterauftragsverarbeiter):

Der Auftragsverarbeiter nutzt für die Ausspielung von Recruiting-Kampagnen Werbeplattformen (z. B. Meta-Plattformen) sowie für WhatsApp-Nachrichten die WhatsApp Business Solution/Cloud API. Diese Anbieter verarbeiten Daten typischerweise zumindest teilweise in eigener datenschutzrechtlicher Verantwortlichkeit nach ihren jeweiligen Bedingungen. Der Verantwortliche stellt die erforderlichen Informationen an Bewerber/Betroffene sicher.

Anlage 3 – Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter implementiert TOMs nach Art. 32 DSGVO, die geeignet sind, ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die nachstehenden Maßnahmen sind praxisorientiert und werden regelmäßig überprüft und bei Bedarf angepasst.

1. Zutrittskontrolle

• Zugriff auf Arbeitsräume nur für berechtigte Personen; Besuchermanagement nach Bedarf

2. Zugangskontrolle (Accounts/Authentifizierung)

• Personalisierte Benutzerkonten
• Starke Passwörter
• Multi-Faktor-Authentifizierung (MFA) in genutzten Systemen, soweit verfügbar
• Sperrung von Zugängen bei Austritt (Offboarding-Prozess)

3. Zugriffskontrolle (Berechtigungen)

• Rollen-/Rechtekonzepte (Need-to-know/Least-Privilege)
• Zugriffsbeschränkung nach System: Perspective (max. 4 Nutzer), Hetzner Uploads (max. 1 Nutzer), Meta Business Manager/WhatsApp (max. 3 Nutzer), Close (max. 4 Nutzer)
• Regelmäßige Rechteprüfung

4. Weitergabekontrolle / Übermittlung

• TLS-verschlüsselte Übertragung (HTTPS/SSL)
• Kontrollierte Weitergabe an den Verantwortlichen (Links/Exports/Benachrichtigungen)
• Keine Weitergabe an unberechtigte Dritte

5. Eingabekontrolle / Nachvollziehbarkeit

• Protokollierung/Logs soweit in den eingesetzten Systemen verfügbar
• Interne Dokumentation wesentlicher Bearbeitungsschritte (z. B. Kampagnenstart/-ende, Löschvorgänge)

6. Verfügbarkeitskontrolle / Backups

• Nutzung der Backup-/Wiederherstellungsfunktionen der eingesetzten Anbieter
• Regelmäßige Updates/Patches der eingesetzten Systeme
• Schutz vor Malware auf Endgeräten nach Stand der Technik

7. Trennungsgebot / Mandantentrennung

• Projekt-/Kampagnentrennung je Verantwortlichem
• Berechtigungen und Ablagestrukturen getrennt je Kunde

8. Endgerätesicherheit / Lokale Daten

• Arbeitsrechner (Windows 11) mit Benutzerpasswortschutz und automatischer Bildschirmsperre
• Lokale Speicherung von Bewerberdaten ist organisatorisch nicht vorgesehen; temporäre Zwischenspeicherungen (z. B. beim Öffnen von Uploads) können technisch bedingt auftreten und werden durch organisatorische Maßnahmen minimiert (z. B. Vermeidung von Downloads, regelmäßige Bereinigung von Download-/Temp-Ordnern).

9. Incident Response / Meldewege

• Interner Prozess zur Erkennung, Bewertung und Behandlung von Sicherheitsvorfällen
• Datenschutzkontakt: datenschutz@wildweiss.com
• Benachrichtigung des Verantwortlichen gemäß § 10