Greifswalder Straße 226
10405 Berlin

IHK: HRB 259653 B
030 81 45 19 68
www.weldersoftware.de
info@weldersoftware.de

Sicherheits und Datenschutzbestimmungen WELDER

Version: Oktober 2023

Inhalt

Kapitel 1 | **Vorwort**

Innerhalb von WELDER erstellen wir enorm attraktive digitale Anwendungen für Mitarbeiter. Mit unserer Plattform können Mitarbeiter und Führungskräfte ganz einfach Entwicklungsgespräche führen, direkt an Unternehmensentwicklungen beteiligt werden oder E-Learnings verfolgen. Auf diese Weise tragen wir zur persönlichen Entwicklung vieler Mitarbeiter bei.

Um dies zu ermöglichen, müssen wir eine Menge Daten speichern und verarbeiten. Das bietet viele Vorteile, bringt aber auch Verantwortung mit sich. Wir bei WELDER sind uns bewusst, dass der Schutz der Privatsphäre vielleicht die größte Herausforderung für unser Unternehmen darstellt.

Wir ergreifen daher umfangreiche Maßnahmen und tun alles, um zu verhindern, dass Daten in falsche Hände geraten. Dabei entscheiden wir uns für eine Vorgehensweise, die in erster Linie auf nachweisbare technische Sicherheit setzt. Die nachweisbaren Maßnahmen liegen in der Architektur unserer Anwendungen. Leider erleben wir immer noch zu oft bürokratische Scheinsicherheit; es gibt umfangreiche Handbücher, Richtlinien und Verfahren, die den Mitarbeitern kaum bekannt sind. Das ist auch der Grund, warum wir unser System in regelmäßigen Abständen von externen Experten prüfen lassen und uns beispielsweise vorerst nicht für eine ISO-Zertifizierung entscheiden. Natürlich haben wir auch entsprechende begleitende Maßnahmen ergriffen.

Dieses Dokument gibt Ihnen einen Einblick in das Gesamtpaket der Maßnahmen, die WELDER zum Thema Datensicherheit und Datenschutz ergreift. Alle WELDER-Mitarbeiter werden darin ausführlich mit einbezogen. Jährlich wird dieses Dokument als fester Punkt in den Jahresplänen von WELDER überprüft.

So stellen wir sicher, dass personenbezogene Daten bei WELDER in sicheren Händen sind. Jetzt und in Zukunft.

Rob Wouters und Maarten Schellekens - Inhaber WELDER bv
Sven Huirne – Geschäftsführer WELDER Software GmbH

Kapitel 2 | **Definitionen**

DSGVO | Die Datenschutz-Grundverordnung (DSGVO) regelt, was mit den persönlichen Daten von Personen gemacht werden darf und was nicht. Bei jeder Verwendung personenbezogener Daten muss die Verletzung der Privatsphäre so gering wie möglich sein.

Kunde | Die Organisation, mit der WELDER Software GmbH einen Vertrag abschließt und die die Software von WELDER nutzt.

Für die Verarbeitung Verantwortlicher | Der für die Verarbeitung Verantwortliche bestimmt die Ziele und Mittel, mit denen personenbezogene Daten verarbeitet werden. Bei einem Vertrag zwischen WELDER und dem Kunden ist der Kunde der Verantwortliche.

Datenverarbeiter | Eine natürliche oder juristische Person, eine Behörde, ein Dienst oder eine andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. In einer Vereinbarung zwischen WELDER und dem Auftraggeber/Kunde ist WELDER der Datenverarbeiter.

Endnutzer | Mitarbeiter eines Auftraggebers, die die WELDER-Software nutzen. Zum Beispiel, um intern Nachrichten auszutauschen, Entwicklungsgespräche vorzubereiten oder ein E-Learning zu absolvieren.

Gesprächszyklus | Alle Momente, in denen Manager mit Mitarbeitern über deren Entwicklung sprechen. Auch HR-Zyklus oder HRM-Zyklus genannt.

WELDER Software | Die digitale Anwendung, die von WELDER entwickelt wurde, um Mitarbeiter einzubinden, zu engagieren, zu trainieren und zu entwickeln.

Entwicklungsgespräch | Ein Gespräch zwischen zwei Endnutzern über z.B. Zufriedenheit, Leistung oder Ambitionen. Diese Gespräche können über die WELDER Software geplant, vorbereitet und aufgezeichnet werden.

E-Learning | Eine digitale Anwendung innerhalb der WELDER Software, in der der Auftraggeber seinen Mitarbeitern (Endnutzern) etwas über ein bestimmtes Thema beibringen möchte.

(1st/2nd) Manager | Der Endnutzer, der einem anderen Endnutzer hierarchisch übergeordnet ist. Diese Person plant z.B. oft die Interviews in einem Interview Zyklus.

Verknüpfung | Die automatische Übernahme von Personaldaten durch WELDER, z.B. aus einem Gehaltsabrechnungspaket.

Kapitel 3 | **Strategische Richtlinien**

3.1 Strategische Richtlinien

Diese Richtlinie beschreibt die internen Sicherheits- und Datenschutzmaßnahmen von WELDER. Diese Richtlinien werden in regelmäßigen Abständen von einer externen Agentur überprüft. Die letzte Prüfung wurde im März 2022 von 'De Functionaris' (CoC: 69175829) durchgeführt. Die Ergebnisse dieser externen Prüfung sind auf Anfrage erhältlich (info@weldersoftware.de).

Es stehen mehrere Dokumente rund um die Sicherheits- und Datenschutzpolitik von WELDER zur Verfügung:

- **Sicherheits- und Datenschutzpolitik** | Gilt als Quelldatei. Die wichtigsten Grundsätze von WELDER sind hier aufgeführt.
- **Datenschutzerklärung WELDER** | Dies ist das, was viele neue Benutzer zu sehen bekommen, wenn sie die Software von WELDER zum ersten Mal benutzen Sie fasst die wesentlichen Punkte der Sicherheits- und Datenschutzpolitik kurz zusammen.
- **Datenverarbeitungsvereinbarung** | Diese enthält spezifische Vereinbarungen zwischen WELDER und dem Auftraggeber auf der Grundlage der Sicherheits- und Datenschutzpolitik von WELDER.
- **Allgemeine Geschäftsbedingungen** | Hier werden die Voraussetzungen für eine Zusammenarbeit zwischen WELDER und dem Auftraggeber geregelt.
- **Verträge für WELDER-Mitarbeiter** | Diese legen die Erwartungen von WELDER in Bezug auf Sicherheit und Datenschutz fest.

3.2 Berechtigungsmodell

Ein Berechtigungsmodell zeigt, welche Mitarbeiter welche Rechte haben. Das untenstehende Berechtigungsmodell zeigt, welche internen/externen Beteiligten von WELDER Zugriff auf welche Daten haben.

	Nutzung der Software	Zugriff auf Datenbank-daten	Vergabe/Änderung von Berechtigungen. WELDER-Mitarbeiter	WELDER-only Funktionen in WELDER-Software	Administrator-rechte in WELDER-Software
Entwicklung WELDER	x	x		x	x
Sonstige Mitarbeiter WELDER	x			x	x
Geschäftsführung WELDER	x	x	x	x	x
Endnutzer KUNDE	x				
Administratoren KUNDE	x				x

Der Datenschutzbeauftragte von WELDER ist dafür verantwortlich, dieses Berechtigungsmodell zu überwachen, bei Abweichungen diese zu melden und gegebenenfalls Anpassungen vorzunehmen.

3.3 Eigentumsrechte an den Daten

Der Kunde ist Eigentümer der Daten und als solcher letztlich dafür verantwortlich, dass die Endnutzer über ihre Rechte in Bezug auf den Datenschutz aufgeklärt werden. Hierfür gibt es drei Möglichkeiten:

- Der Kunde hat bereits in seinen Arbeitsverträgen mit seinen Mitarbeitern darüber informiert;
- Der Kunde verwendet eine separate Datenschutzerklärung, die er selbst verfasst (möglicherweise auf der Grundlage der Vorlage am Ende dieses Dokuments);
- Der Kunde verwendet eine von WELDER zur Verfügung gestellte Datenschutzerklärung.

Darüber hinaus schließen WELDER und die Kunden eine Datenverarbeitungsvereinbarung ab, in der die Verwendung der Daten und die Rechte der Nutzer beschrieben werden.

3.4 Rollen und Verantwortlichkeiten

Es ist wichtig, intern die richtige Rollenverteilung für den Schutz personenbezogener Daten zu kennen. Nachstehend finden Sie eine Auflistung der Mitarbeiter mit diesbezüglichen Verantwortlichkeiten.

Betroffene Person/en WELDER	Rolle/Verantwortung
Beauftragter für den Schutz der Privatsphäre/Datenschutzbeauftragter (2023: Ferry van Hooydonk)	Meldung von Abweichungen von der Datenschutzpolitik. Er hält die Datenschutzpolitik auf dem neuesten Stand. Berichterstattung an die Geschäftsleitung über die Einhaltung der Datenschutzpolitik.
Entwickler WELDER	Verwaltung und Entwicklung technischer Maßnahmen zum Schutz der Privatsphäre.
Kundenbetreuer WELDER	Kommunikation mit Kunden im Zusammenhang mit der Datenschutzpolitik.
Geschäftsführung WELDER bv (Rob Wouters, Maarten Schellekens) Geschäftsführung WELDER Software GmbH (Sven Huirne)	Letztlich verantwortlich für den Datenschutz.

Alle WELDER-Mitarbeiter erhalten bei Arbeitsantritt eine Schulung zum digitalen Datenschutz. Danach erhält jeder Mitarbeiter einmal im Jahr eine Datenschutzschulung. Die Inhalte werden vom Datenschutzbeauftragten vorbereitet.

3.5 IT-Nutzung und soziale Medien

Die Richtlinien für die Nutzung von IT-Ressourcen und sozialen Medien sind im Arbeitsvertrag mit jedem Mitarbeiter von WELDER festgelegt.

3.6 Budget

Die Geschäftsleitung ist dafür verantwortlich, dass ein ausreichendes Budget zur Verfügung gestellt wird, um die Maßnahmen dieser Sicherheits- und Datenschutzpolitik einzuhalten. Sollte das Budget nicht ausreichen, ist dies der Geschäftsleitung durch den Datenschutzbeauftragten mitzuteilen.

3.7 Daten- und Dokumentenaustausch

Wenn personenbezogene Daten von Endnutzern des Auftraggebers/Kunden an WELDER geliefert werden, ist es die Pflicht aller Mitarbeiter, dafür zu sorgen, dass diese über das eigens dafür eingerichtete Dokumentenportal hochgeladen werden. Der Datenschutzbeauftragte erhält hierüber einen Hinweis, kann beurteilen, ob es sich um die richtigen Daten handelt und leitet diese an den zuständigen Kundenbetreuer weiter. Auf diese Weise verhindern wir, dass diese personenbezogenen Daten bei Personen landen, für die sie nicht bestimmt sind.

3.8 Erlaubnis für Bildmaterial

Jeder Mitarbeiter von WELDER hat in seinem Arbeitsvertrag festgehalten, dass aufgezeichnetes Bildmaterial des Mitarbeiters in der externen Kommunikation verwendet werden darf.

3.9 Passwort-Richtlinie

WELDER betreibt eine Single Sign On Policy über Google. Jeder Mitarbeiter von WELDER ist aufgefordert, dieses bei Dienstantritt zu nutzen und ein eindeutiges Passwort zu generieren. Es ist nicht erlaubt, ein Passwort zu verwenden, das man sich persönlich merken kann; es muss ein Passwortmanager, nämlich Bitwarden, verwendet werden. Allen WELDER-Mitarbeitern wird empfohlen, das Google-Passwort vierteljährlich zu ändern.

3.10 Evaluierung der Richtlinien

Diese Richtlinien werden einmal jährlich durch den Datenschutzbeauftragten von WELDER evaluiert und in Absprache mit der Geschäftsleitung von WELDER aktualisiert.

Kapitel 4 | **Verarbeitungsregister**

4.1 Tätigkeiten

WELDER übt die folgenden Tätigkeiten aus, die die Verarbeitung der Daten umfassen von :

- Kunden, die die WELDER-Software nutzen (4.2)
- Rekrutierung / Auswahl / Personalverwaltung (4.3)
- Marketing / Vertrieb / CRM (4.4)
- Finanzielle Verwaltung (4.5)

Wer welche Verantwortung für die einzelnen Tätigkeiten trägt, welche Daten mit welcher Absicht erhoben werden, wie sie beschafft werden und ob es sich um sensible personenbezogene Daten handelt, wird im Folgenden für jede Tätigkeit dargelegt.

4.2 Kunden, die die WELDER-Software nutzen

Im Folgenden werden die Grundsätze beschrieben, die im Zusammenhang mit der Hauptaktivität von WELDER angewandt werden: Kunden, die die WELDER-Software nutzen.

4.2.1 Verantwortliche Parteien

Wenn WELDER einen Vertrag mit einem Kunden abschließt, um die Software von WELDER den Endnutzern des Kunden zur Verfügung zu stellen, ist der Kunde der für die Datenverarbeitung Verantwortliche und WELDER der Auftragsverarbeiter.

4.2.2 Personenbezogene Daten

Die zu erfassenden personenbezogenen Daten werden pro Kunde festgelegt. Dabei gilt: so wenig wie möglich. Es werden nur die personenbezogenen Daten erhoben, die für die Erbringung der Dienstleistungen erforderlich sind. Nachfolgend finden Sie eine Übersicht über die personenbezogenen Daten, die erhoben werden können, einschließlich einer Begründung, warum sie notwendig sind.

Persönliche Daten	Grund
Name	Erforderlich, um zu wissen, um welchen Endnutzer es sich handelt und um ihn z.B. im E-Mail-Verkehr ansprechen zu können.
E-Mail	Erforderlich, um zu wissen, um welchen Endnutzer es sich handelt und um ihn z.B. im E-Mail-Verkehr ansprechen zu können.
Geburtsdatum	Notwendig, damit die Endbenutzer einander zum Geburtstag gratulieren können, und manche Kunden entscheiden sich für ein Entwicklungsgespräch rund um einen Geburtstag.
Eintrittsdatum	Erforderlich, damit Endbenutzer eingeladen werden können, an einem digitalen Einarbeitungsprogramm teilzunehmen oder einen Fragebogen auszufüllen.

Datum des Dienstausstieges	Notwendig, damit der Endbenutzer zu einem Exit-Interview oder einem Fragebogen eingeladen werden kann.
Funktion	Erforderlich, damit Endnutzer sehen können, welche Kompetenzen von einer Position erwartet werden, oder wenn der Kunde z. B. einen Interviewzyklus oder ein E-Learning segmentieren möchte und nur Endnutzer mit einer bestimmten Position dazu einladen will.
Abteilung	Erforderlich, damit ein Kunde z.B. in einem Gesprächszyklus oder E-Learning segmentieren kann und nur Endnutzer aus einer bestimmten Abteilung dazu einladen möchte.
1e Manager	Notwendig, damit bekannt ist, wer ein Entwicklungsgespräch mit dem Endnutzer führen darf und wer Einblick in die persönliche Entwicklung von welchen Endnutzern haben darf.
2e Manager	Erforderlich, damit bekannt ist, wer ein Entwicklungsgespräch mit dem Endnutzer führen darf und wer Einblick in die persönliche Entwicklung von welchen Endnutzern haben darf.
Organisatie	Erforderlich, damit der Endnutzer das Gehalt mit seinem Vorgesetzten bei einem Entwicklungsgespräch besprechen kann.
Gehalt	Erforderlich, damit der Endnutzer das Gehalt mit seinem Vorgesetzten bei einem Entwicklungsgespräch besprechen kann.
Gehaltsskala	Erforderlich, damit der Endnutzer das Gehalt mit seinem Vorgesetzten bei einem Entwicklungsgespräch besprechen kann.
Gehaltsstufe	Erforderlich, damit der Endnutzer das Gehalt mit seinem Vorgesetzten bei einem Entwicklungsgespräch besprechen kann.
Rufnummer	Erforderlich, damit die Endnutzer einander schnell per Telefon erreichen können.
Sprache	Erforderlich, damit klar ist, in welcher Sprache die WELDER-Software angezeigt werden soll.

Ein Kunde kann zusätzliche personenbezogene Daten vom Endnutzer anfordern. Dabei handelt es sich dann um einige personenbezogene Daten, die ein Mitarbeiter selbst eingibt und die Erlaubnis zur Verarbeitung erteilt.

4.2.3 Beschaffung von persönlichen Daten

WELDER erhält diese persönlichen Daten von den Kunden auf verschiedene Weise.

- Der Endanwender gibt diese Informationen selbst in die WELDER-Software ein
- Der Auftraggeber stellt WELDER diese Informationen zur Verfügung

● Es wird eine automatische Verbindung mit einem vom Kunden bereits verwendeten Softwaresystem hergestellt
Die beste Methode wird im gegenseitigen Einvernehmen für jeden Kunden festgelegt. Wenn personenbezogene Daten übermittelt werden, geschieht dies niemals per E-Mail, sondern über eine gesondert eingerichtete Online-Umgebung, die dem Datenschutzbeauftragten von WELDER zur Verfügung gestellt wird. Auf diese Weise begrenzen wir das Risiko, dass ein Mitarbeiter versehentlich eine E-Mail weiterleitet.

4.3 Rekrutierung / Auswahl / Personalverwaltung

Die Grundsätze der Anwerbung, Auswahl und Personalverwaltung werden im Folgenden beschrieben. Mit anderen Worten: alle (potenziellen) Mitarbeiter von WELDER.

4.3.1 Verantwortliche Person

In diesem Fall ist WELDER für die Verarbeitung von (personenbezogenen) Daten verantwortlich.

4.3.2 Persönliche Daten

Von potenziellen Mitarbeitern werden nur Name, Lebenslauf und E-Mail-Adresse und/oder Telefonnummer gespeichert. Der Lebenslauf dient der Beurteilung, ob der Bewerber über ausreichende Erfahrung für die zu besetzende Stelle verfügt, und die Kontaktdaten dienen der Kontaktaufnahme mit dem Bewerber. Von aktuellen Mitarbeitern werden die folgenden Daten erhoben:

Persönliche Daten	Motivation
Adresse, Postleitzahl, Ort	Um einen Brief (z. B. eine Geburtstagskarte) an die Heimatadresse zu senden. Und um den Pendelverkehr einzurichten.
Rufnummer	Zur Kontaktaufnahme.
Private E-Mail Adresse	Um per Post zu kommunizieren, solange die Geschäftspostadresse noch nicht aktiviert ist.
BSN / Sozialversicherungsnummer	Zur Identifizierung
IBAN	Um das Gehalt zu überweisen.

4.2.4 Beschaffung von personenbezogenen Daten

WELDER erhält diese personenbezogenen Daten, indem er sie von dem betreffenden (potenziellen) Arbeitnehmer anfordert. Dieser (potenzielle) Mitarbeiter gibt seine Zustimmung zur Verwendung der Daten.
Es kann auch die Erlaubnis erteilt werden, Bilder in sozialen Medien zu verwenden, z. B. für eine Marketingkampagne.

4.4 Marketing / Vertrieb / CRM

Im Folgenden werden die Grundsätze beschrieben, die im Zusammenhang mit den Marketing- und Verkaufsaktivitäten von WELDER angewandt werden.

4.4.1 Verantwortliche Partei
In diesem Fall ist WELDER für die Verarbeitung der (personenbezogenen) Daten verantwortlich.

4.4.2(Persönliche) Daten
Die folgenden Daten werden im Rahmen der Marketing- und Vertriebsaktivitäten von WELDER erhoben.

(Persönliche) Daten	Motivation
Website besuchen	Zur Überwachung der Anzahl der Website-Besucher auf der Grundlage der IP-Adresse.
Auffindbarkeit der Seiten	Zur Verbesserung der SEO-Leistung
Klicks auf Anzeigen	Zur Überwachung der Ergebnisse von (Google-)Anzeigen.
Name des Unternehmens	Um Sie im Falle einer Demo-Anfrage zu kontaktieren
Name	Um Sie im Falle einer Demo-Anfrage zu kontaktieren
Anzahl der Mitarbeiter	Um zu wissen, wie groß die betreffende Organisation ist
Rufnummer	Um Sie im Falle einer Demo-Anfrage zu kontaktieren
E-Mail Adresse	Um Sie im Falle einer Demo-Anfrage zu kontaktieren
Funktion	Um Sie im Falle einer Demo-Anfrage zu kontaktieren
Gehaltspaket	Um zu wissen, wo wir eine mögliche Verbindung herstellen können
E-Mail-/Telefonverkehr	Um andere WELDER-Kollegen über den Kontakt mit diesem Kunden zu informieren

4.4.3 Beschaffung von personenbezogenen Daten
Website-Traffic, Auffindbarkeit und Anzeigenklicks werden automatisch von Softwareprogrammen (Google Analytics, Semrush, Google Ads) generiert. Dies ist vorerst anonym.
Wenn eine Demo-Anfrage geplant ist oder ein Kontaktformular ausgefüllt wird, werden einige Kontaktdaten abgefragt. Auch hier wird auf diese Datenschutz- und Sicherheitsrichtlinien verwiesen. Alle Kontakte mit potenziellen Neukunden werden im CRM-Paket von WELDER (Hubpot) gespeichert.

4.5 Finanzverwaltung
Im Folgenden werden die Grundsätze beschrieben, die im Zusammenhang mit den auf die Finanzverwaltung ausgerichteten Aktivitäten von WELDER angewandt werden.

4.5.1(Persönliche) Daten
Die folgenden Daten sind den Finanzunterlagen von WELDER entnommen.

(Persönliche) Daten	Motivation
IBAN-Lieferant	Um Geld an unsere Lieferanten zu überweisen
IBAN Kunde	Für eine mögliche Gutschriftrechnung
Kostenstelle Kunde	Für die Kundenverwaltung

Adressdaten des Kunden	Für jegliche Kommunikation per Post
E-Mail Adresse des Kunden	Für die administrative Kommunikation
Kundenzahlungen	Für eventuelle Zahlungserinnerungen

4.5.2 Beschaffung von personenbezogenen Daten
Die Kundendaten werden vom Kunden angefordert. Dabei wird auch angegeben, wofür diese Daten benötigt werden. Alle erhaltenen Daten werden in der Fakturierungssoftware von WELDER erfasst.
Die Zahlungsdaten werden automatisch durch das Verwaltungsprogramm von WELDER verarbeitet.

4.6 Sensible personenbezogene Daten
Die von WELDER erhobenen personenbezogenen Daten fallen unter die Kategorie der "gewöhnlichen personenbezogenen Daten". Die gehaltsbezogenen personenbezogenen Daten können als "sensible personenbezogene Daten" bezeichnet werden, und WELDER macht seine Mitarbeiter darauf aufmerksam, dass beim Umgang mit diesen personenbezogenen Daten besondere Diskretion geboten ist.

4.7 Unterauftragsverarbeiter
WELDER hat derzeit einen Unterauftragsverarbeiter (Hetzner in Deutschland als Hosting-Partner) und garantiert, dass dieser Unterauftragsverarbeiter ein entsprechendes Verarbeitungsverzeichnis mit Kontaktangaben führt.

4.8 Rechtmäßigkeit der Verarbeitung
Im AVG sind sechs Grundlagen aufgeführt, die die Rechtmäßigkeit der Verarbeitung personenbezogener Daten beschreiben:

1. Sie haben die Erlaubnis der betroffenen Person
2. Die Verarbeitung der Daten ist für die Erfüllung eines Vertrags erforderlich
3. Die Verarbeitung der Daten ist notwendig, weil Sie gesetzlich dazu verpflichtet sind.
4. Die Verarbeitung der Daten ist notwendig, um lebenswichtige Interessen zu schützen.
5. Die Verarbeitung der Daten ist für die Wahrnehmung einer Aufgabe von öffentlichem Interesse oder einer öffentlichen Behörde erforderlich
6. Die Verarbeitung der Daten ist zur Verfolgung Ihres berechtigten Interesses erforderlich

Grundsätzlich geht WELDER bei allen Aktivitäten von der Basis 1: Zustimmung aus. Bei der erstmaligen Nutzung wird jeder Endnutzer mittels eines Pop-up-Fensters auf eine Datenschutzerklärung aufmerksam gemacht, die auf diese Sicherheits- und Datenschutzpolitik verweist. Der Endnutzer kann die Plattform nur nutzen, wenn er dem zustimmt und damit die Verarbeitung personenbezogener Daten erlaubt.

Der Endnutzer hat jederzeit das Recht, diese Zustimmung zu widerrufen, was mit einer E-Mail an info@weldersoftware.de geschehen kann. Dies wird in der Datenschutzerklärung erklärt.

Die Zustimmung muss vom Endnutzer aus freien Stücken gegeben werden; ein Endnutzer darf nicht an der Erfüllung des Arbeitsvertrags gehindert werden, wenn er sich weigert. Dies wird den Kunden von WELDER mitgeteilt.

Es gibt Kunden, die in ihren Arbeitsverträgen mit den Endnutzern klare Vereinbarungen über die Verwendung von Unternehmenssoftware getroffen haben. In diesem Fall kann Basis 2 (Vertrag ausführen) gewählt werden und es erscheint kein Pop-up bei der ersten Benutzung der WELDER Software. Die richtige Basis wird pro Kunde bestimmt.

Kapitel 5 | **Technische Ausrüstung**

5.1 Dienst-/Anwendungsarchitektur
WELDER bietet eine Cloud-Lösung, um in das Lernen, die Entwicklung, das Engagement und die Bindung der Mitarbeiter zu investieren.

5.2 Anzahl der aktiven Nutzer
Am 1. April 2022 wird die Zahl der WELDER-Nutzer rund 47.000 betragen.

5.3 Datenschutz durch Technik und Datenschutz durch Voreinstellung
Datenschutz durch Technik und Datenschutz durch Voreinstellungen sind zwei verbindliche Grundsätze der Datenschutz-Grundverordnung (DSGVO). Privacy by Design" bedeutet, dass der Datenschutz bereits bei der Entwicklung eines Produkts oder einer Dienstleistung berücksichtigt wird. Datenschutz durch Voreinstellungen bedeutet, dass die Standardeinstellungen so datenschutzfreundlich wie möglich sein sollten.
Die Entwicklungsabteilung von WELDER wird regelmäßig in diesen Prinzipien geschult, und diese Prinzipien werden bei jeder Entwicklung angewendet.

5.4 Beendigung/Konkurs
Sollte WELDER aus welchem Grund auch immer aufhören zu existieren, wird der Auftraggeber vom Auftragnehmer rechtzeitig darüber informiert. In diesem Fall ist der Auftragnehmer/Kunde verpflichtet, die Software für mindestens 1 Monat nach der Beendigung weiterzuführen und den Code danach an den Auftraggeber zu übergeben. Auftraggeber und Auftragnehmer haben nach Beendigung des Vertrages keine weiteren finanziellen Verpflichtungen gegenüber dem anderen.

5.5 Beendigung
Bei Kündigung des Dienstes durch den Kunden hat dieser das Recht, die Nutzerdaten vernichten zu lassen.

5.6 Unterstützung und Helpdesk
Der inhaltliche Support für Mitarbeiter des Auftraggebers geht zu Lasten des Auftraggebers. Die Unterstützung von Mitarbeitern des Auftraggebers bei technischen Fehlern geht zu Lasten des Auftragnehmers. Beispiel: Einem Mitarbeiter, der sein Passwort vergessen hat oder eine Aktivierungs-E-Mail in seinem Spam-Filter verschwinden sieht, wird vom Auftraggeber geholfen. Wenn die automatisch generierte E-Mail der Option "Passwort vergessen" nicht funktioniert, wird dies vom Auftragnehmer behoben.
Hauptansprechpartner für alle Mitarbeiter bezüglich der Nutzung der Plattform ist der Auftraggeber. Wenn der Auftraggeber einen technischen Fehler vermutet, kann der Auftragnehmer per E-Mail kontaktiert werden.
Der Auftragnehmer antwortet dem Kunden innerhalb von 24 Stunden auf technische Fehler und behebt sie innerhalb von 5 Arbeitstagen.
Der Auftragnehmer steht mit einer oder wenigen Kontaktpersonen des Auftraggebers in Verbindung und kommuniziert nicht direkt mit anderen Mitarbeitern des Auftraggebers.

5.7 Problem- und Störungsmanagement
Tritt eine Störung auf, so wird sie so schnell wie möglich gemäß den Leitlinien in Artikel 6 des Vorschlags behoben und kann direkt in die Produktionsumgebung übernommen werden.

5.8 Änderungsmanagement
Jede Änderung am System wird in der Versionskontrolle (GIT) festgehalten. Nach jeder Änderung werden automatisch alle Testfälle ausgeführt. Erst wenn alle Tests erfolgreich verlaufen sind, wird die Änderung in die Abnahmeumgebung überführt. Dort werden alle manuellen Tests noch vom Auftragnehmer durchgeführt. Nach der Freigabe kann die exakte Software aus der Abnahmeumgebung per Knopfdruck in die Produktionsumgebung verschoben werden. Im unwahrscheinlichen Fall von Fehlern in der Produktionsumgebung kann mit einem Knopfdruck die vorherige Version wiederhergestellt werden.

5.9 Kapazitätsmanagement
Die Server, auf denen die Software läuft, werden kontinuierlich und automatisch überwacht. Bevor Kapazitätsprobleme auftreten, löst diese Software Warnungen an die Mitarbeiter von WELDER aus. Wenn sich abzeichnet, dass ein Kapazitätsmangel droht, wird die Kapazität rechtzeitig erhöht.

5.10 Verfügbarkeitsmanagement
Mehrere Uptime-Monitore überprüfen kontinuierlich die Verfügbarkeit verschiedener Komponenten. Sobald diese nicht mehr verfügbar sind, wird automatisch eine Meldung an die Mitarbeiter von WELDER gesendet. Die Empfänger von WELDER ergreifen dann die entsprechenden Maßnahmen.

5.11 Kontinuitätsmanagement
WELDER analysiert regelmäßig, ob es Risiken gibt, die die Kontinuität der Software gefährden, und informiert den Kunden rechtzeitig. Das gesamte System wird täglich gesichert. In regelmäßigen Abständen werden diese Sicherungen getestet, um sicherzustellen, dass sie funktionieren.

5.12 Identitäts- und Berechtigungsmanagement
WELDER wird nur Mitarbeitern des Auftraggebers die Nutzung der Software ermöglichen. Die Art und Weise, wie dies am effizientesten geschehen kann, wird während des Auftrags festgelegt.

5.13 Wiederherstellungspunkt-Ziel (RPO)
Jede Nacht wird ein Backup erstellt, wobei der maximale Datenverlust einen Tag beträgt. Nach Vereinbarung kann dieser Zeitraum verkürzt werden.

5.14 Ziel Wiederherstellungszeit
Wird in regelmäßigen Abständen getestet. Die tatsächliche Wiederherstellungszeit liegt innerhalb von 24 Stunden.

5.15 Berichtsoptionen
Die Nutzung der Plattform kann analysiert werden. Entsprechende Screenshots sind in diesem Vorschlag enthalten.

5.16 Verwaltung/Patching von Schwachstellen
Jede Nacht wird geprüft, ob neue Patches für das Betriebssystem verfügbar sind. Wenn diese verfügbar sind, werden sie automatisch installiert. Externe Softwarekomponenten werden regelmäßig auf Sicherheitspatches überprüft.

5.17 Benutzerkonten / Passwortpolitik
Jeder Benutzer hat ein Konto mit einem Passwort. Passwörter werden mit einem „Salt“ und mit einem Einweg-Hash (Bcrypt) gespeichert. Single Sign On mit Client-Systemen wird weiter koordiniert. Im Falle von Single Sign On ist die Speicherung von Passwörtern möglicherweise nicht erforderlich.

5.18 Benutzerrechte
Auf technischer Ebene: Zugang zum Server nur für WELDER-Entwickler.
Im CMS: Vom Prinzip her können bestimmte Personen mit Administratorrechten ausgestattet werden und Benutzerrechte zuweisen.

5.19 Sicherheitsgrundlagen/Absicherung
WELDER verwendet Standard-OS-Sicherheitspatches. Keine zusätzliche Absicherung.

5.20 Pensionierung von Mitarbeitern WELDER
Der Zugang zum Server erfolgt über SSH-Schlüssel. Beim Ausscheiden aus dem Unternehmen wird der öffentliche Schlüssel des betreffenden Mitarbeiters entfernt.

5.21 Ausscheiden von Mitarbeitern Kunden
Wenn ein Benutzer aus dem Dienst ausscheidet (basierend auf dem definierten Ausscheidungsdatum), wird das Konto gelöscht und der Benutzer kann sich nicht mehr anmelden.

5.22 Überwachung
Wenn die Website offline geht, werden Meldungen generiert. Der Zugriff auf den Server ist nur von IP-Adressen möglich, die auf der Whitelist stehen. Andere IP-Adressen werden von der Firewall blockiert.

5.23 Anti-Malware und Viren
Die Software läuft unter Linux, wobei ein aktives Patch-Management das Risiko von Viren oder Malware verringert. Darüber hinaus läuft die gesamte Software isoliert in Docker-Containern. Dadurch wird sichergestellt, dass alle Prozesse vollständig isoliert sind und die Folgen von Malware oder Viren begrenzt sind.

5.24 Zugang zu den Endnutzern
Durch Herunterladen der Anwendung über den App Store (iOS) oder den Play Store (Android) oder durch Zugriff in einem Webbrowser über eine zu vereinbarende Subdomain von welder.de. Das übliche Szenario variiert von Kunde zu Kunde.

5.25 Verschlüsselte Daten
Alle Daten werden sowohl "im Ruhezustand" als auch während der Übertragung verschlüsselt. Bei der Übertragung werden die Daten über https verschlüsselt.

5.26 Lagerung innerhalb der EU
Hetzner-Rechenzentrum in Falkenstein. Die Speicherung/Verarbeitung innerhalb der EU wird garantiert.

Kapitel 6 | **Datenschutz-Folgenabschätzung (DPIA)**

Von: WELDER
Bewilligungszeitpunkt: Mai 2022

Eine Datenschutzfolgenabschätzung wird alle zwei Jahre durchgeführt, um zu prüfen, ob die derzeitigen Maßnahmen noch ausreichend sind. Wenn sich strukturelle Fragen ändern, z.B. wenn sich die Anzahl/Art der verarbeiteten personenbezogenen Daten oder die Zusammenarbeit mit Unterauftragsverarbeitern erheblich ändert, kann eine häufigere Durchführung dieser Datenschutzfolgenabschätzung beschlossen werden. Sie wird dann intern vom Datenschutzbeauftragten von WELDER durchgeführt, möglicherweise unter der Beratung/Anleitung eines externen Beraters. Die unten aufgeführten Kapitel 1 bis 6 gelten als die Hauptkapitel bei der Durchführung dieser Datenschutzfolgenabschätzung.

6.1 Die verantwortliche Partei

Bei Vereinbarungen mit Kunden ist WELDER der Verarbeiter und der Kunde der Verantwortliche.

6.2 Verarbeitung von personenbezogenen Daten und Rechtmäßigkeit

Kategorie der personenbezogenen Daten:	Personenbezogene Daten von Kunden, Lieferanten, Mitarbeitern und anderen Personen
Kategorie der Interessenvertreter:	Mitarbeiter
Grundlage für die Verarbeitung:	Rechtsgrundlage 1: Der Verarbeiter hat die Einwilligung der betroffenen Person zur Verarbeitung der Daten. Jede betroffene Person muss ihre ausdrückliche Zustimmung erteilen vor der Nutzung der Systeme des Auftragsverarbeiters
Zweck der Verarbeitung:	Der Auftragsverarbeiter verarbeitet personenbezogene Daten, für die er verantwortlich ist, da dies einerseits der betroffenen Person bei der persönlichen Entwicklung hilft und andererseits Erkenntnisse zur Verbesserung der strategischen Personalplanung liefert
Standort des Verarbeiters:	's-Hertogenbosch, die Niederlande
Aufbewahrungsfrist:	Die Daten werden ohne Enddatum gespeichert. WELDER vereinbart mit jedem Kunden, ob die Daten nach einer bestimmten Zeit gelöscht werden. Ohne ausdrückliche Aufforderung des Auftraggebers ist dies ohne ein Enddatum. Wenn ein Mitarbeiter

	(betroffene Person) eines Kunden (für die Verarbeitung Verantwortlicher) um die Löschung personenbezogener Daten verlangt, wird dies stets beachtet
Sicherheitsmaßnahmen:	Siehe Kapitel 2 und 4

6.3 Art der Verarbeitung

WELDER sammelt personenbezogene Daten auf drei Arten.

a) In einigen Fällen wird eine **automatische Verbindung** mit dem Personalregistrierungssystem eines Kunden hergestellt. In diesem Fall werden z. B. der Name und die E-Mail-Adresse des Mitarbeiters auf der Plattform von WELDER registriert.

b) Darüber hinaus kann ein Mitarbeiter **seine eigenen Informationen eingeben**. Zum Beispiel gibt ein Mitarbeiter Informationen über seine Hobbys an oder lädt ein Profilbild oder eine Telefonnummer hoch. Diese Informationen werden von WELDER gespeichert.

c) Schließlich werden auch bestimmte Aktionen der Mitarbeiter **unter der Oberfläche aufgezeichnet**. Zum Beispiel Informationen darüber, wann sich jemand eingeloggt hat oder welche Seiten er besucht hat. Diese Informationen können WELDER helfen, die Software jedes Mal zu verbessern, und dem Kunden, Erkenntnisse zu gewinnen.

6.4 Speicherung von personenbezogenen Daten

WELDER stellt sicher, dass die Daten in den Datenbanken des Hosting-Providers Hetzner in Deutschland gespeichert werden. Das Design dieser Datenbanken wird von den Entwicklern von WELDER gestaltet und von externen Prüfern unabhängig getestet.

6.5 Bedarf für die Verarbeitung

Verschiedene personenbezogene Daten haben ihre eigene Notwendigkeit. Einige personenbezogene Daten werden aus praktischen Erwägungen heraus erhoben. Zum Beispiel können wir einem Mitarbeiter ohne E-Mail-Adresse keine Einladung zu einer Mitarbeiterbefragung schicken. Andere personenbezogene Daten werden erhoben, um die richtigen Erkenntnisse für die strategische Personalplanung zu gewinnen. So werden z. B. Führungskräfte gebeten, Informationen über das geschätzte Potenzial von Mitarbeitern zu liefern, die für automatische Analysen durch das Management des Kunden verwendet werden. Schließlich werden personenbezogene Daten verarbeitet, um die Mitarbeiter bei ihrer persönlichen Entwicklung zu unterstützen. Zum Beispiel kann ein Mitarbeiter bei der Vorbereitung einer Leistungsbeurteilung Einblick in seine persönliche Arbeitszufriedenheit geben. Diese Daten müssen gesammelt und verarbeitet werden, damit Vorgesetzte und Mitarbeiter während des Gesprächs gemeinsam einen Aktionsplan für die persönliche Entwicklung der Mitarbeiter erstellen können.

6.6 Bewertung der Risiken bei der Verarbeitung

Bei der Risikobewertung gibt es zwei wichtige Aspekte: 1) die Wahrscheinlichkeit, dass Daten nicht ordnungsgemäß verarbeitet werden, und 2) die Auswirkungen dessen, was passieren könnte, wenn diese Daten nicht ordnungsgemäß verarbeitet werden.

WELDER schätzt die Wahrscheinlichkeit, dass Daten nicht ordnungsgemäß verarbeitet werden, als relativ gering ein. Dies liegt daran, dass viele technische Maßnahmen ergriffen wurden (Kapitel 2) und dass diese Maßnahmen von einer externen Stelle unabhängig geprüft werden (Kapitel 4). Es ist gut zu wissen, was passiert, wenn unerwartete Daten nicht richtig verarbeitet werden. Das wahrscheinlichste Szenario ist, dass ein Prozess gegenüber einem Mitarbeiter unterbrochen wird. Zum Beispiel erhält ein Mitarbeiter keine E-Mail. Oder eine Information geht verloren und muss neu eingegeben werden. Die Auswirkungen sind dann relativ gering und betreffen oft nur einen Mitarbeiter. In einem eher unwahrscheinlichen Szenario werden die Daten Dritten zugänglich. Personaldaten gelangen zum Beispiel in die Hände von Hackern oder kommerziellen Einrichtungen. In einer Auswirkungsskala von niedrig-mittel-hoch schätzen wir die Auswirkungen dann auf "mittel". Einerseits landen dann viele Daten "auf der Straße". Andererseits stufen wir die verarbeiteten Daten nicht als besonders datenschutzsensibel ein. Die von WELDER verarbeiteten personenbezogenen Daten sind beispielsweise weniger datenschutzsensibel als etwa Bankkontodaten oder medizinische Daten.

6.7 Beschreibung der vorgeschlagenen Maßnahmen

Alle WELDER-Mitarbeiter werden im Rahmen des Einführungsprogramms über alle Sicherheits- und Datenschutzmaßnahmen aufgeklärt. Darüber hinaus werden alle neuen Entwicklungen in regelmäßigen Besprechungen erörtert. Und es ist ein fester Bestandteil der Jahresplanung von WELDER. Darüber hinaus werden auch weiterhin regelmäßige externe Tests durchgeführt, um etwaige "blinde Flecken" aufzuspüren.

Kapitel 7 | **Externer Test von Computest**

WELDER lässt in regelmäßigen Abständen einen externen Test zum Thema Sicherheit durch ein externes Unternehmen durchführen. Die aktuellen Ergebnisse sind für alle Kunden öffentlich zugänglich. Der letzte Scan* wurde von der Firma Computest durchgeführt und erfolgte im Rahmen der offiziellen Partnerschaft mit dem Softwareunternehmen AFAS.
**Test abgenommen in unserer niederländischen Niederlassung WELDER BV. Bei Fragen wenden Sie sich bitte an info@weldersoftware.de.*

Computest arbeitet mit Farbkodierung:

- Rot: abgelehnt
- Orange: einige verbesserungsbedürftige Bereiche, neue Prüfung in einem Jahr
- Grün: in gutem Zustand, neues Audit in 3 Jahren

Bei der letzten Überprüfung am 25. März 2022 wurde die grüne Punktzahl erreicht, was WELDER die Gewissheit gibt, dass die Datensicherheit und der Datenschutz gut gesichert sind.

WELDER

Computest

Partner Security Quickscan
WELDER B.V.

>>

WE EAT SECURITY FOR BREAKFAST.

25 maart 2022
Michael de Klein

Samenvatting

Op 23 en 24 maart 2022 heeft Computest een security quickscan uitgevoerd voor WELDER. Hiervoor heeft Michael de Klein, securityspecialist bij Computest, gesproken met Rob Wouters en Stefan Boenders, ontwikkelaars bij WELDER, over de beveiliging van de WELDER HRM applicatie. Ook heeft Computest kort gekeken naar de broncode van de applicatie en een korte securitytest uitgevoerd.

Het doel van een quickscan is om een idee te geven van de staat van beveiliging van de WELDER HRM applicatie. Dit document geeft dan ook alleen een algemene indruk, en is geen volledige opsomming van alle kwetsbaarheden in de applicatie.

De WELDER HRM applicatie biedt bedrijven een omgeving waarin het sociale aspect centraal staat. In de applicatie kunnen middels een berichtenbord berichten gedeeld worden met collega's en leidinggevenden. Verder bevat de applicatie de mogelijkheid om competenties te koppelen aan medewerkers en deze competenties te toetsen door middel van een functioneringsgesprek, welke allemaal gedocumenteerd kunnen worden binnen het platform. Verder biedt het platform ook de mogelijkheid om e-learning modules te maken welke gebruikt kunnen worden voor bijvoorbeeld on- of off-boarding doeleinden of andere kennisdeling doeleinden. Middels een marktplaats module is het voor medewerkers mogelijk om voorwerpen, diensten of doelen te delen binnen een organisatie, of punten toe te kennen aan goede doelen.

De applicatie gebruikt werknemer data uit het AFAS-systeem om bijbehorende accounts aan te maken binnen het platform, zodat iedere (nieuwe) werknemer hier toegang toe heeft. Daarnaast is het mogelijk na het afronden van een gesprek om hiervan een verslag op te slaan bij een werknemer in het AFAS-systeem.

Resultaat

Op basis van de vier onderstaande pijlers zijn scores toegekend. Verder in dit document lichten wij elke onderwerp nader toe:

Scoreverdeling	
Security in het ontwikkelproces	
Security in code	
Security in de praktijk	
Risico voor AFAS	

Het risico voor AFAS heeft een groen stoplicht gekregen. AFAS verwacht dat er na 3 jaar een vervolgafspraak wordt gemaakt.

Security in het ontwikkelproces

Er is ruimte voor verbetering voor security in het ontwikkelproces.

Computest heeft gesproken met ontwikkelaars van WELDER over de ontwikkeling van de HRM applicatie. Hieruit is gebleken dat op veel onderdelen in het ontwikkelproces er aandacht is voor security gezien de omvang van het team, maar dat er nog wel een aantal verbeteringen mogelijk zijn. Binnen WELDER zijn er op het moment vier ontwikkelaars werkzaam, welke allemaal aan dezelfde applicatie werken. De applicatie is gebouwd met een AngularJS front-end en Python Pyramid als back-end framework, en is gebouwd als multi-tenant omgeving. De achterliggende database bevat alle data van alle WELDER-klanten en wordt op data-niveau van elkaar onderscheiden. Bij het inrichten van omgevingen voor nieuwe klanten wordt er gevraagd naar de AFAS-token van de klant, waarvoor geen vastgestelde procedure is opgesteld naar hoe de klant dit token zou moeten aanleveren.

Omdat alle ontwikkelaars werken aan dezelfde applicatie en daarom ook allemaal gebruik maken van dezelfde diensten (infrastructuur, databases, ed.) is hierin geen onderscheid gemaakt in wie toegang heeft tot welke componenten. Wel wordt er op de servers afgedwongen dat enkel IP-adressen van ontwikkelaars in combinatie met '*SSH Public key authentication*' mogen verbinden naar de servers.

Op de GitLab code repository wordt veel aandacht besteed aan code kwaliteit en peer reviewing. Zo worden nieuwe functies ontwikkeld in een aparte branch en worden er code reviews uitgevoerd worden op alle nieuwe merge requests om alle toegevoegde code te beoordelen. Er is echter geen proces dat dit afdwingt, maar wordt gedaan op eigen initiatief van de ervaren ontwikkelaars. Daarnaast worden er in de deployment pipeline tests uitgevoerd op de code, en worden dependencies van de software gescand op publiek bekende kwetsbaarheden. Alle interne accounts (tot bijvoorbeeld de broncode) zijn beschermd met een Google SSO oplossing welke Multi-factor authenticatie (2FA) afdwingt. Door deze maatregelen is het ontwikkelproces voldoende beschermd. Wel is er een klein risico doordat alle ontwikkelaars in het team toegang hebben tot de productieomgeving van de applicatie. Als een aanvaller toegang weet te krijgen tot het systeem van een van deze ontwikkelaars, is het mogelijk dat de aanvaller daarmee toegang tot de productieomgeving weet te krijgen. Daarnaast is er geen proces waarmee WELDER controleert of de systemen van de ontwikkelaars voldoende beveiligd zijn, door bijvoorbeeld te controleren of updates zijn geïnstalleerd, disk encryptie aanstaat en of een virusscanner actief is.

Op basis van bovenstaande informatie adviseert Computest:

- Richt een proces in waarmee inzicht verkregen kan worden in de beveiliging van alle werkstations;
- Stel een procedure in voor het ontvangen van AFAS-tokens, bijvoorbeeld versleuteld per mail met het wachtwoord per sms;
- Isoleer databases van elkaar zodat er bij een security kwetsbaarheid extra isolatie aanwezig is tussen klanten;
- Sla het AFAS-token versleuteld op in de database zodat deze bij een lek niet uitgelezen en/of misbruikt kan worden;
- Beperk het aantal personen dat toegang heeft tot de productie-infrastructuur.

Security in code

Er is voldoende aandacht voor security in de broncode van de applicatie(s).

Computest heeft samen met de ontwikkelaar van WELDER gekeken naar de broncode van de HRM applicatie. De applicatie is geschreven in Python in combinatie met het Pyramid framework. Dit wordt gedaan op een overzichtelijke wijze, en alle code wordt zo geschreven dat de functionaliteiten en waarden zichzelf zo helder mogelijk omschrijven. Alle externe softwarepakketten die worden ingeladen worden in de CI/CD pipeline gecontroleerd op publiekelijk bekende kwetsbaarheden en de teststraat zal falen wanneer deze aangetroffen worden. Alle routes binnen de applicatie worden op object niveau ingeladen en hier worden ook authenticatie checks op een gecentraliseerde manier afgehandeld.

Voor communicatie met de database wordt gebruik gemaakt van het softwarepakket *sqlalchemy* dat gebruik maakt van '*Object-relational mapping (ORM)*' waardoor er geen gebruik gemaakt hoeft te worden van SQL-queries. Hiermee biedt het *sqlalchemy* softwarepakket beveiliging tegen SQL-injectie.

Ook is er structureel bescherming aanwezig tegen '*Cross-Site Scripting (XSS)*' doordat hiervoor in zowel de front- als back-end gebruik gemaakt wordt van functies die gebruikersinvoer filteren. In combinatie met deze beschermende maatregelen heeft WELDER ook een zeer stricte '*Content Security Policy (CSP)*' ingesteld zodat er in het geval van een incidentele XSS-kwetsbaarheid een extra laag van bescherming aanwezig is.

Verder lijkt er geen bescherming geboden te worden tegen '*Cross-Site Request Forgery (CSRF)'.* Er worden bij POST-verzoeken geen gebruik gemaakt van CSRF-tokens waardoor het voor een aanvaller mogelijk zou zijn om een dergelijke aanval uit te voeren. Tijdens de code review heeft Computest deze kwestie besproken met de ontwikkelaar, welke aangaf dat er beschermd wordt tegen CSRF door op het sessie-cookie de '*Same-Site*' vlag een '*Lax*' waarde mee te geven. Omdat er in een aantal gevallen toch een sessie-cookie meegestuurd zal worden bij een Lax Same-Site waarde, heeft Computest ook deze uitzonderingen onderzocht samen met de ontwikkelaar. Hieruit is geconcludeerd dat er in eerste oogopslag geen sprake is van uitzonderingsgevallen waarin een CSRF aanval toch reëel zou zijn. Omdat Same-site nog niet overal ondersteund wordt adviseert Computest toch een extra CSRF-beschermingsmaatregel te overwegen.

Op basis van het bovenstaande adviseert Computest:

- Onderzoek de implementatie van CSRF-tokens in de applicatie om een extra laag van bescherming in te bouwen tegen Cross-Site Request Forgery aanvallen;
- Documenteer de codebase zodat deze voor nieuwe en de huidige ontwikkelaars beter te begrijpen is;
- Bouw in de bestaande CI/CD pipeline SAST en/of DAST tools in zodat hier ook op applicatie niveau beter inzicht verkregen wordt op het security-niveau.

Security in de praktijk

Er is voldoende aandacht voor security in de praktijk.

Tijdens het assessment heeft Computest het securityniveau van de WELDER HRM applicatie beoordeeld. Computest is van mening dat de omgeving voldoende beveiligd is, maar ziet op enkele plekken ruimte voor verbetering om het securityniveau verder te verhogen.

Tijdens de demo van de applicatie heeft Computest bevonden dat er AFAS-tokens onversleuteld worden getoond in het configuratie interface van de applicatie. Computest adviseert om dit token enkel gemaskeerd of helemaal niet te tonen in de applicatie, en deze in de database versleuteld op te slaan.

Hoewel er in de code structureel bescherming aanwezig is tegen XSS-kwetsbaarheden, heeft Computest op twee plekken in de applicatie toch een incidentele XSS-kwetsbaarheid aangetroffen. Beide kwetsbaarheden zijn aangetroffen in het formulier waar managers functioneringsgesprekken in documenteren, allereerst in de velden waar managers opmerkingen achter kunnen laten bij een behaald doel, en daarnaast in de pop-up die getoond wordt wanneer een manager het formulier wilt opslaan en de naam van de medewerker getoond wordt. Hoewel Computest geen werkende '*Proof-of-Concept*' heeft van een mogelijke exploitatie, is deze bevinding tijdens het assessment gecommuniceerd met WELDER die dit zal controleren en oplossen. Computest adviseert om de applicatie te controleren op het tonen van gebruikersinvoer om te valideren dat alle incidentele XSS-kwetsbaarheden opgelost zijn.

Risico voor AFAS

Het securityrisico voor AFAS wordt ingeschat op 'Laag'.

De WELDER HRM applicatie maakt gebruik van werknemer data uit AFAS voor het aanmaken van accounts in de omgeving, en zal enkel bij het afronden van een vastgelegd gesprek een gespreksverslag terug uploaden naar AFAS.

In de applicatie heeft Computest geen kritieke kwetsbaarheden aangetroffen en heeft ook geen verdere aanleiding gevonden om te geloven dat de confidentialiteit, integriteit of beschikbaarheid van het AFAS-token, dan wel data afkomstig uit AFAS, op enig manier geschaad kan worden. Computest schat het risico voor AFAS daarom in op 'laag'.

Computest
always on.

info@computest.nl
+31(0)88 733 13 37
www.computest.nl

We zijn een team van gepassioneerde en ervaren technisch specialisten die applicaties en infra-struc-turen optimaal laten werken. Wij geloven in geïntegreerde quality assurance en bieden daarom diensten op het gebied van performance, security en functionele testautomatisering.

In alles wat we doen worden we gedreven door een grenzeloze passie voor kwaliteit. Daarom werken we voor iedere sector samen in kleine, gespecialiseerde agile teams. Daarmee houden we de lijnen kort zodat we de beste resultaten behalen.

Kapitel 8 | **Externe Überprüfung durch den Beauftragten**

Zusätzlich zu einer technischen Prüfung der funktionalen Sicherheitsmaßnahmen lässt WELDER seine Richtlinien regelmäßig extern auf Datenschutz und politische Maßnahmen prüfen. Das letzte Audit wurde im Juli 2023 von der in Capelle a/d Ijssel ansässigen Agentur De Functionaris (KvK 6915829) durchgeführt. Diese Agentur ist auf Datenschutzgesetze (AVG/ DSGVO) spezialisiert. Durch die regelmäßige Durchführung dieser beiden externen Prüfungen stellt WELDER sicher, dass die richtigen Maßnahmen getroffen wurden, um die Sicherheit der Daten von (Mitarbeitern von) Kunden zu gewährleisten. Bei Fragen kontaktiere bitte info@weldersoftware.de.

Kapitel 9 | **Verarbeitervereinbarung**

Fassung September - 2022

Vereinbarung mit dem Verarbeiter: _____
Datum: _____
Vertragsparteien:
1. _____, mit Sitz in _____
unter der Adresse _____, eingetragen im Handelsregister unter der Nummer_____, vertreten durch _____
im Folgenden als **"für die Verarbeitung Verantwortlicher"** bezeichnet,

und

2. WELDER Software GmbH mit Sitz in (10405) Berlin an der Adresse Greifswalder Straße 226, eingetragen im Handelsregister unter der Nummer HRB 259653 B und hiermit rechtsgültig vertreten durch S.A-J.M Huirne, der auch in eigenem Namen unterschreibt; nachstehend: "**Verarbeiter**" genannt

Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter werden im Folgenden auch gemeinsam als **"Parteien" bezeichnet**;

in Erwägung nachstehender Gründe:
Die Parteien haben eine Vereinbarung in Bezug auf _____ geschlossen (im Folgenden als "**Vereinbarung**" bezeichnet). Im Rahmen der Erfüllung unserer Vereinbarung werden personenbezogene Daten verarbeitet.

Diese Vereinbarung führt dazu, dass der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter möchten in dieser Vereinbarung die Rechte und Pflichten für die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß den Bestimmungen von Artikel 28 Absatz 3 der Datenschutz-Grundverordnung festlegen.

Artikel 1. Definitionen

Die unten und oben verwendeten Begriffe ergeben sich aus der Allgemeinen Datenschutzverordnung und haben die folgende Bedeutung:

1.1. **Personenbezogene Daten** sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person (**"betroffene Person"**); als bestimmbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren

besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

1.2. **Verarbeitung**: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten oder einer Reihe personenbezogener Daten wie das Erheben, das Speichern, die Organisation, die Strukturierung, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;

1.3. **Betroffene Person**: identifizierte oder identifizierbare natürliche Person, auf die sich die personenbezogenen Daten beziehen;

1.4. **Auftragsverarbeitervereinbarung**: bezeichnet diese Vereinbarung einschließlich ihrer Anhänge ("**Auftragsverarbeitervereinbarung**");

1.5. **Vereinbarung**: die Hauptvereinbarung, aus der sich diese Verarbeitungsvereinbarung ergibt;

1.6. **Verletzung des** Schutzes **personenbezogener Daten**: eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete Daten führt ("**Datenverletzung**");

1.7. **Datenschutz-Folgenabschätzung:** Durchführung einer Abschätzung der Auswirkungen der geplanten Verarbeitungstätigkeiten auf den Schutz personenbezogener Daten vor der Durchführung der Verarbeitung;

1.8. **Aufsichtsbehörde**: eine unabhängige öffentliche Behörde, die für die Überwachung der Einhaltung der Gesetze in Bezug auf die Verarbeitung personenbezogener Daten zuständig ist. In den Niederlanden ist dies die Behörde für personenbezogene Daten;

1.9. **AVG**: die Allgemeine Datenschutzverordnung *(2016/679/EU)*;

1.10. **Datenschutzgesetze**: alle geltenden Datenschutzgesetze und -vorschriften, einschließlich, aber nicht beschränkt auf das AVG und DSGVO.

Artikel 2. Entstehung, Dauer und Beendigung

2.1. Diese Verarbeitungsvereinbarung tritt an dem Tag in Kraft, an dem die Vertragsparteien sie unterzeichnen.

2.2. Diese Auftragsverarbeiter-Vereinbarung wird auf unbestimmte Zeit geschlossen und endet zum Zeitpunkt der Beendigung der Vereinbarung.

2.3. Im Falle der Beendigung des Auftragsverarbeitervertrages überträgt der Auftragsverarbeiter alle personenbezogenen Daten an den Auftragsverarbeiter oder vernichtet auf ausdrückliche schriftliche Aufforderung des Auftragsverarbeiters die im Besitz des Auftragsverarbeiters befindlichen personenbezogenen Daten.

2.4. Verpflichtungen, die ihrer Natur nach auch nach Beendigung der Auftragsverarbeitervereinbarung fortbestehen sollen, bleiben auch nach der

Beendigung bestehen. Zu diesen Verpflichtungen gehören Bestimmungen über Vertraulichkeit, Weitergabe und Vernichtung, Haftung und anwendbares Recht.

Artikel 3. Verarbeitung personenbezogener Daten

3.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen auf der Grundlage seiner schriftlichen Anweisungen und unter seiner Verantwortung und auf die im Vertrag festgelegte Weise.

3.2. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur im Auftrag des für die Verarbeitung Verantwortlichen, es sei denn, es gelten andere rechtliche Verpflichtungen.

3.3. Der Auftragsverarbeiter hat keine Kontrolle über den Zweck und die Mittel der Verarbeitung personenbezogener Daten und trifft keine Entscheidungen über die Verwendung personenbezogener Daten, die Weitergabe an Dritte und die Dauer der Speicherung personenbezogener Daten.

3.4. Der Auftragsverarbeiter hat den für die Verarbeitung Verantwortlichen unverzüglich schriftlich zu benachrichtigen, wenn eine Anweisung nach angemessener Auffassung des Auftragsverarbeiters gegen geltende Datenschutzgesetze verstößt.

3.5. Auf Anfrage des Auftragsverarbeiters stellt dieser alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in dieser Auftragsverarbeitervereinbarung festgelegten Verpflichtungen nachzuweisen.

3.6. Der Auftragsverarbeiter stellt sicher, dass die Bedingungen für die Verarbeitung personenbezogener Daten gemäß den geltenden Datenschutzvorschriften eingehalten werden.

3.7. Der Auftragsverarbeiter gewährt seinen Mitarbeitern nur insoweit Zugang zu personenbezogenen Daten, als dies für die Erbringung der vertragsgemäßen Leistungen erforderlich ist. Der Auftragsverarbeiter stellt sicher, dass seine Mitarbeiter einer Geheimhaltungsklausel unterliegen.

3.8. Der Auftragsverarbeiter darf personenbezogene Daten außerhalb des EWR nur mit vorheriger schriftlicher Zustimmung des für die Verarbeitung Verantwortlichen verarbeiten.

Artikel 4. Sicherung persönlicher Daten

4.1. Der Auftragsverarbeiter trifft alle geeigneten technischen und organisatorischen Maßnahmen, um personenbezogene Daten gegen Verlust oder jede Form der unrechtmäßigen Verarbeitung zu schützen. Diese Maßnahmen gewährleisten ein angemessenes Sicherheitsniveau unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie unter Berücksichtigung der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung und der nach Wahrscheinlichkeit und Schweregrad unterschiedlichen Risiken, die die Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter für die Rechte und Freiheiten der betroffenen Personen darstellt. Die umgesetzten Sicherheitsmaßnahmen sind im Anhang (Sicherheitsdatenschutzerklärung WELDER) zu finden.

4.2. Der Auftragsverarbeiter informiert den Auftragsverarbeiter, wenn sich die Sicherheitsmaßnahmen ändern.

4.3. Der Verantwortliche des Auftragsverarbeiters gestattet dem Auftragsverarbeiter, die Einhaltung der Sicherheitsmaßnahmen durch den Auftragsverarbeiter zu überprüfen oder auf Antrag des Auftragsverarbeiters die Datenverarbeitungseinrichtungen des Auftragsverarbeiters durch eine vom Auftragsverarbeiter zu benennende Untersuchungsstelle im Zusammenhang mit den unter diese Vereinbarung fallenden Verarbeitungstätigkeiten überprüfen zu lassen. Die verantwortliche Partei des Auftragsverarbeiters stellt sicher, dass die Untersuchungsstelle verpflichtet ist, ihre Ergebnisse gegenüber Dritten vertraulich zu behandeln.

4.4. Der Auftragsverarbeiter trägt alle Kosten, Gebühren und Auslagen im Zusammenhang mit der Inspektion, einschließlich angemessener interner Kosten, die dem Auftragsverarbeiter entstehen.

4.5. Der für die Verarbeitung Verantwortliche übermittelt dem Verarbeiter eine Kopie des Inspektionsberichts.

Artikel 5. Weitergabe von personenbezogenen Daten an Dritte

5.1. Der Auftragsverarbeiter darf personenbezogene Daten nur auf ausdrückliche schriftliche Anordnung des Auftragsverarbeiters oder auf Anordnung einer Justiz- oder Verwaltungsbehörde an Dritte weitergeben oder zugänglich machen, vorausgesetzt, dass der Auftragsverarbeiter in einem solchen Fall den Auftragsverarbeiter so schnell wie möglich nach Erhalt einer solchen Anordnung benachrichtigt, damit der Auftragsverarbeiter die ihm zur Verfügung stehenden Rechtsmittel ausüben kann.

5.2. Der Auftragsverarbeiter muss den Verantwortlichen schriftlich um Erlaubnis bitten, personenbezogene Daten an Dritte weiterzugeben, und darf dies nur nach schriftlicher Zustimmung des Verantwortlichen tun.

5.3. Ist der Auftragsverarbeiter der Ansicht, dass er einer zuständigen Behörde aufgrund einer rechtlichen Verpflichtung personenbezogene Daten zur Verfügung stellen muss, so tut er dies erst nach Rücksprache mit der für die Verarbeitung Verantwortlichen und deren schriftlicher Zustimmung. Er unterrichtet den Auftragsverarbeiter so bald wie möglich schriftlich über die rechtliche Verpflichtung und übermittelt alle relevanten Informationen, die der Auftragsverarbeiter vernünftigerweise benötigt, um die erforderlichen Maßnahmen zu ergreifen, damit er entscheiden kann, ob und unter welchen Bedingungen eine Offenlegung erfolgen kann.

Artikel 6. Ersuchen von betroffenen Personen

6.1. Der Auftragsverarbeiter unterrichtet den Auftragsverarbeiter über alle direkt von den betroffenen Personen eingegangenen Anträge bezüglich der Rechte der betroffenen Personen gemäß den geltenden Datenschutzgesetzen, einschließlich, aber nicht beschränkt auf Anträge auf Einsichtnahme, Berichtigung, Löschung, Einschränkung der

Verarbeitung oder Übertragung personenbezogener Daten. Der Auftragsverarbeiter kommt einem solchen Ersuchen nur dann nach, wenn er von der betroffenen Person schriftlich dazu aufgefordert wurde.

6.2. Der Auftragsverarbeiter ist verpflichtet, alle Auskunftsersuche an den Auftragsverarbeiter im Zusammenhang mit der Verarbeitung personenbezogener Daten unverzüglich und ordnungsgemäß im Sinne des AVG zu bearbeiten.

Artikel 7. Kooperationsprozessor

Der Auftragsverarbeiter arbeitet mit dem für die Verarbeitung Verantwortlichen bei der Durchsetzung seiner Verpflichtungen zusammen:

i. auf Anfragen von betroffenen Personen bezüglich der Ausübung ihrer Rechte nach den geltenden Datenschutzgesetzen zu reagieren;
ii. geeignete technische und organisatorische Maßnahmen ergreifen, um ein risikoadäquates Sicherheitsniveau zu gewährleisten;
iii. Meldung von Datenschutzverletzungen an Aufsichtsbehörden und betroffene Personen;
iv. um eine Datenschutz-Folgenabschätzung durchzuführen;
v. vor jeder Verarbeitung, die ein hohes Risiko birgt, die Aufsichtsbehörde zu konsultieren.

Artikel 8. Einschaltung von Unterauftragsverarbeitern nach Auftragsverarbeiter

Der Auftragsverarbeiter kann einen Unterauftragsverarbeiter mit der Durchführung dieser Auftragsverarbeitervereinbarung beauftragen. Wird ein Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Auftragsverarbeiters beauftragt, so hat der Auftragsverarbeiter diesem Unterauftragsverarbeiter vertraglich mindestens die gleichen Verpflichtungen in Bezug auf die Verarbeitung und den Schutz personenbezogener Daten aufzuerlegen wie die in dieser Auftragsverarbeitungs-vereinbarung enthaltenen Verpflichtungen. Bevor der Auftragsverarbeiter einen Unterauftragsverarbeiter hinzufügt/ersetzt, teilt er dies dem Auftragsverarbeiter schriftlich mit und gibt ihm die Möglichkeit, gegen diese Änderung Einspruch zu erheben. Zum Zeitpunkt des Abschlusses dieser Auftragsverarbeitungsvereinbarung ist der Auftragsverarbeiter berechtigt, die in der Liste (Sicherheits- und Datenschutzrichtlinie WELDER) aufgeführten Unterauftragsverarbeiter zu beauftragen. Der Auftragsverarbeiter ist in jeder Hinsicht verantwortlich und haftbar für die Handlungen und Unterlassungen von Dritten, die er im Rahmen dieser Auftragsverarbeitervereinbarung beauftragt.

Artikel 9. Geheimhaltung

Der Auftragsverarbeiter garantiert, dass er personenbezogene Daten und andere von dem für die Verarbeitung Verantwortlichen erhaltene Informationen streng vertraulich behandelt. Der Auftragsverarbeiter darf die vom Auftragsverarbeiter erhaltenen personenbezogenen Daten und sonstigen Informationen nur an Personen weitergeben, verteilen, zur Verfügung stellen oder anderweitig offenlegen, die nicht seine Mitarbeiter sind, welche die vom

Auftragsverarbeiter erhaltenen personenbezogenen Daten und sonstigen Informationen zum Zwecke ihrer Arbeit für den Auftragsverarbeiter kennen müssen, und er darf diesen Mitarbeitern nur dann Zugang zu den vom Auftragsverarbeiter erhaltenen personen-bezogenen Daten und sonstigen Informationen gewähren, wenn sie über die Vertraulichkeit der vom Auftragsverarbeiter erhaltenen personenbezogenen Daten und sonstigen Informationen informiert wurden. Der Auftragsverarbeiter hat die Bestimmungen dieser Vereinbarung auch seinen Mitarbeitern aufzuerlegen.

Artikel 10. Datenschutzverletzung

10.1. Der Auftragsverarbeiter ist verpflichtet, den Auftragsverarbeiter so schnell wie möglich, spätestens jedoch 24 Stunden, nachdem der Auftragsverarbeiter davon Kenntnis erlangt hat, über jede Sicherheitsverletzung (gleich welcher Art) zu informieren, die sich (teilweise) auf die Verarbeitung personenbezogener Daten bezieht oder beziehen könnte.

10.2. In jedem Fall muss der Verarbeiter dem Verarbeiter Informationen über Folgendes zur Verfügung stellen:

i. die Art des Verstoßes, wenn möglich unter Angabe der Kategorien der betroffenen Personen und der ungefähren Anzahl der betroffenen Personen;

ii. die (potenziell) betroffenen personenbezogenen Daten und ungefähr die Anzahl der betroffenen personenbezogenen Daten;

iii. die festgestellten und erwarteten Folgen der Verletzung für die Verarbeitung personenbezogener Daten und die betroffenen Personen; und

iv. die Maßnahmen, die der Auftragsverarbeiter ergriffen hat und ergreifen wird, um den Verstoß zu beheben, gegebenenfalls einschließlich der Maßnahmen zur Abmilderung etwaiger negativer Folgen des Verstoßes.

10.3. Der Auftragsverarbeiter erkennt an, dass er unter Umständen gesetzlich verpflichtet ist, den betroffenen Personen und/oder Behörden eine Sicherheitsverletzung (gleich welcher Art) zu melden, die sich (teilweise) auf die vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten bezieht oder beziehen könnte. Eine solche Meldung durch den Auftragsverarbeiter gilt nicht als Verletzung dieser Auftragsverarbeiter-Vereinbarung oder des Vertrags oder anderweitig als unrechtmäßige Handlung.

10.4. Der Auftragsverarbeiter ergreift alle erforderlichen Maßnahmen, um den (möglichen) Schaden einer Sicherheitsverletzung zu begrenzen, und unterstützt den Auftragsverarbeiter bei der Benachrichtigung der betroffenen Personen und/oder Behörden.

Artikel 11. Haftung

11.1. Die Haftung des Auftragsverarbeiters beschränkt sich auf unmittelbare Schäden, die sich aus der Nichteinhaltung dieser Auftragsverarbeiter-Vereinbarung ergeben oder damit zusammenhängen, oder auf Handlungen, die gegen die geltenden Datenschutzgesetze verstoßen.

11.2. Der Auftragsverarbeiter haftet nicht für Schäden, die durch die unsachgemäße Verwendung durch den Auftragsverarbeiter verursacht werden, oder für Schäden, die anderweitig durch den Auftragsverarbeiter verursacht werden.

11.3. Die Haftung des Auftragsverarbeiters für vom Auftragsverarbeiter erlittene Schäden und/oder verwirkte Geldbußen im Sinne von Artikel 11.1 ist pro Ereignis (wobei eine zusammenhängende Reihe von Ereignissen als ein einziges Ereignis gilt) auf Schadensersatz bis zu einem Betrag von höchstens 50.000 € beschränkt. In keinem Fall darf die gesamte und kumulative Haftung einer Partei gegenüber der anderen Partei im Rahmen und im Zusammenhang mit der Vereinbarung 500.000 € übersteigen.

Artikel 12. Schlussbestimmungen

12.1. Diese Auftragsverarbeitervereinbarung ist Teil der Vereinbarung. Alle Rechte und Pflichten aus der Vereinbarung gelten daher auch für die Verarbeitungsvereinbarung.

12.2. Im Falle eines Widerspruchs zwischen den Bestimmungen der Verarbeitungsvereinbarung und der Vereinbarung sind die Bestimmungen dieser Verarbeitungsvereinbarung maßgebend.

12.3. Abweichungen von dieser Verarbeitungsvereinbarung sind nur gültig, wenn sie schriftlich vereinbart werden.

12.4. Diese Auftragsverarbeiter-Vereinbarung unterliegt dem niederländischen Recht.

12.5. Für alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag ergeben, ist ausschließlich das zuständige Gericht in 's-Hertogenbosch zuständig.

Anhang: Sicherheits- und Datenschutzpolitik WELDER (Version Aug 2023)

So vereinbart und von uns unterzeichnet:

Controller:

Unterzeichnet für und im Namen von: _____

Name: _____

Funktion: _____

Datum und Ort: _____

Unterschrift:

Prozessor:

Unterzeichnet für und im Namen von: WELDER Software GmbH
Namen: Sven Albert-Jan Maria Huirne
Position: Geschäftsführung
Datum und Ort: _____

Unterschrift
S.A-J.M. Huirne

Kapitel 10 | **Erklärung zum Datenschutz**

Wie bereits beschrieben, ist der Auftraggeber von WELDER der für die Datenverarbeitung Verantwortliche. Als für die Datenverarbeitung Verantwortlicher ist der Kunde verpflichtet, seine Mitarbeiter ordnungsgemäß über die Datenschutzrechte zu informieren. Und die Mitarbeiter müssen der Verarbeitung personenbezogener Daten ausdrücklich zustimmen (Grundlage 1).

Es gibt drei Möglichkeiten, wie der Kunde dies tun kann, und WELDER weist seine Kunden bei jeder Zusammenarbeit auf diese drei möglichen Wege hin:

Option 1: Der Auftraggeber nimmt einen Passus in seinen Arbeitsvertrag auf, der mehr darüber aussagt. Der Arbeitnehmer gibt sein Einverständnis, indem er den Vertrag unterschreibt.

Option 2: Der Kunde erstellt eine Datenschutzerklärung und teilt sie jedem Mitarbeiter mit, der die WELDER-Plattform nutzen möchte. Der Mitarbeiter muss dieser Datenschutzerklärung zustimmen, um die Plattform nutzen zu können.

Option 3: Der Kunde verwendet die Standard-Datenschutzerklärung von WELDER. Dies funktioniert technisch genauso wie Option 2, aber da WELDER die Erfahrung gemacht hat, dass viele Unternehmen darauf nicht vorbereitet sind, wurde ein Muster erstellt. Dieses Muster ist unten zu finden.

Bei jeder Zusammenarbeit wird entschieden, welche Option für den Kunden am besten geeignet ist. Bei den Optionen 2 und 3 erhält jeder Mitarbeiter bei der ersten Nutzung der WELDER-Plattform ein automatisches Pop-up-Fenster, das ihn auf seine Datenschutzrechte hinweist. Der Mitarbeiter kann dann seine Zustimmung zur Datenverarbeitung geben oder nicht. Der Kunde erhält einen Überblick darüber, welche Personen ihre Zustimmung gegeben haben und welche nicht.

Datenschutzerklärung <Name des Kunden>

Zum Zwecke der Datenübermittlung um <kunde>.weldersoftware.de

1. Einleitung

<Auftraggeber> legt Wert auf den Schutz der Privatsphäre seiner Mitarbeiter. Auf der Website <kunde>.weldersoftware.de. werden Nutzerdaten gesammelt. Um Klarheit darüber zu schaffen, wie die Privatsphäre von Unternehmen und Mitarbeitern auf der Website geschützt wird, wurde diese Datenschutzerklärung verfasst.

Die Website <kunde>.weldersoftware.de wird z.B. für folgende Zwecke verwendet:
-intern kommunizieren
-interner Befragung der Mitarbeiter
- Durchführung von Entwicklungsgesprächen
-angebotene E-Learnings
-Wissen teilen
- Begleitung der Mitarbeiter bei ihrer persönlichen Entwicklung
<Nichtzutreffendes streichen>

2. Welche Daten werden gespeichert?

Die folgenden Daten werden verarbeitet:

- Vor- und Nachname;
- E-Mail-Adresse (Kommunikation mit der betroffenen Person)
- Funktion (um die Zuständigkeiten mit der Funktion der betroffenen Person zu verknüpfen)
- Geburtsdatum (um einen Geburtstag anzuzeigen)
- Vorgesetzter (um zu wissen, mit wem der Beschwerdeführer ein Fortschrittsgespräch führt)
- (möglicherweise) Zweiter Manager
- Abteilung (um auswählen zu können, ob ein Interviewzyklus für die betroffene Person gilt)
- Datum des Dienstantritts (um ein Jubiläum anzuzeigen)
- Datum des Ausscheidens aus dem Dienst (um einen Benutzer zu entfernen)
- Gehalt (zur Angabe des Gehalts in einer Fortschrittsbesprechung)
- FTE (zur Angabe des Gehalts in einem Vorstellungsgespräch)
- Gehaltstabelle (zur Beratung bei Gehaltsänderungen)
- Selbstinitiierte Bewertungen durch die betroffene Person zu Themen wie Arbeitszufriedenheit, Kompetenzen und Ziele. (Um dem Vorgesetzten und dem Mitarbeiter die Möglichkeit zu geben, ein Gespräch über die Leistung des Mitarbeiters zu führen)

3. Warum werden diese Daten gespeichert?

Verschiedene personenbezogene Daten haben ihre eigene Notwendigkeit. Einige personenbezogene Daten werden aus praktischen Erwägungen heraus erhoben. Zum Beispiel können wir einem Mitarbeiter ohne E-Mail-Adresse keine Einladung zu einer Mitarbeiterbefragung schicken. Andere personenbezogene Daten werden erhoben, um die richtigen Erkenntnisse für die strategische Personalplanung zu gewinnen. So

werden z. B. Führungskräfte gebeten, Angaben zum geschätzten Potenzial ihrer Mitarbeiter zu machen, die für automatische Analysen durch das Management der Kunden verwendet werden. Schließlich werden personenbezogene Daten verarbeitet, um die Mitarbeiter bei ihrer persönlichen Entwicklung zu unterstützen. Beispielsweise kann ein Mitarbeiter bei der Vorbereitung einer Leistungsbeurteilung Einblick in seine persönliche Arbeitszufriedenheit geben. Diese Daten müssen gesammelt und verarbeitet werden, damit Vorgesetzte und Mitarbeiter während des Gesprächs gemeinsam einen Aktionsplan für die persönliche Entwicklung der Mitarbeiter erstellen können.

Lieferant der Plattform <Name der Plattform> ist WELDER.

Name	WELDER
Handelskammer	84324627
Branche	Beratungsorganisation
Anschrift	Mangaan 4B, 5234 GD 's-Hertogenbosch
E-Mail	info@welder.nl
Website	www.welder.nl
Telefon	073-2082800

<Auftraggeber> hat mit WELDER Vereinbarungen über die Verarbeitung personenbezogener Daten getroffen. Diese sind in einem Verarbeitungsvertrag festgehalten, der per E-Mail an info@weldersoftware.de angefordert werden kann. Die Daten aus der Nutzung von <Name Plattform> werden beim Hoster Hetzner in Deutschland gespeichert.

4. Wie lange werden Ihre personenbezogenen Daten aufbewahrt?

Die Nutzungsdaten werden auf den Servern von WELDER für die Dauer des Vertrages mit <Name des Kunden> gespeichert. <Name des Kunden> hat mit WELDER vereinbart, dass personenbezogene Daten, die älter als <Zeitraum> sind, gelöscht werden. <Löschen, was nicht zutrifft>

5. Was sind Ihre Rechte?

Betroffene Personen, Mitarbeiter von <Name Auftraggeber>, haben verschiedene Rechte in Bezug auf Daten. In dieser Datenschutzerklärung informiert <Name Auftraggeber> Sie über Ihre Datenschutzrechte bei der Nutzung von <Name Plattform>. Darüber hinaus haben Sie das Recht, die in <Name Plattform> verarbeiteten personenbezogenen Daten einzusehen oder eine Kopie davon zu erhalten. Gibt es Fehler im System? Dann haben Sie das Recht, diese ändern zu lassen. Wenn es keine Gründe (mehr) für die Aufbewahrung bestimmter Daten gibt, haben Sie das Recht, diese Daten löschen zu lassen. Ein Antrag auf Einsicht, Änderung, Löschung oder Kopie kann an info@welder.nl / <Kontaktdaten Kunde> gerichtet werden.

Schließlich erinnert <Name des Kunden> Sie an die Möglichkeit, eine Beschwerde bei der Behörde für personenbezogene Daten einzureichen.

6. Sicherheit

<Name des Kunden> nimmt den Schutz Ihrer Daten ernst und ergreift geeignete Maßnahmen, um Missbrauch, Verlust, unbefugtem Zugriff, unerwünschter Offenlegung und unbefugter Änderung entgegenzuwirken. Wenn Sie den Eindruck haben, dass die Daten nicht ordnungsgemäß gesichert sind oder es Anzeichen für einen Missbrauch gibt, können Sie die Sicherheits- und Datenschutzpolitik von WELDER anfordern. Diese ist unter www.weldersoftware.de frei abrufbar.

7. Fragen

Wenn Sie Fragen zu dieser Datenschutzerklärung haben, wenden Sie sich bitte an info@weldersoftware.de / Kontaktangaben Kunde>.