DATENSCHUTZ-FOLGENABSCHÄTZUNG			
Projekt (Datenverarubeitung)	Mitarbeiter Portal	**Verantwortliche Stelle**	Verallia Deutschland AG
Bericht Nr.	202102	**Datenschutzbeauftragter**	Thomas Emmendörfer
Ausfertigungsdatum	22.07.2021	**Projektverantwortlicher**	Cornelia Banzhaf (PR Manager); Elisa Sauter (Specialist Communication & CSR);Saskia Müller (DPM)
Aktualisiert am	00.00.0000	**Auftragsverarbeiter**	WOB AG und Microsoft

L1	L2	L3	L4	Fragen	DS-GVO	Antwort
A				**BESCHREIBUNG DER DATENVERARBEITUNG**	**Art. 35/7/a**	
	A1			**Beschreibung der Verarbeitung**	**(90)**	
		A11		**Art der Verarbeitung**	**Q. 1.1**	Verarbeitung von personnenbezogenen Date für den Zugriff auf die Mitarbeiterplattform. Auf der Verallia Mitarbeiterplattform werden allgemeine Informationen zum Unternehmen allen Mitarbeiterinnen und Mitarbeitern der Verallia Deutschland AG zur Verfügung gestellt.
		A12		**Gegenstand der Verarbeitung**	**Q. 1.2**	Besserer Informationsaustausch besonders mit Mitarbeiterinnen und Mitarbeitern ohne Verallia-Mailadresse.
		A13		**Zweck der Verarbeitung**	**Q. 1.3**	Interne Verbreitung von Mitarbeiter relevante Informationen. Informationen werden mit allen Mitarbeiterinnen und Mitarbeitern geteilt. Insbesondere auch eine bessere Erreichbarkeit der Werke und damit der Mitarbeiter ohne Verallia-Mailadresse.
	A2			**Datenkategorien**		E-mail Adresse, personalnummer, passwort
		A21		**Kategorien personenbezogener Daten**	**Q. 1.9**	Es werden personenbezogene Daten von Mitarbeitern verarbeitet.
			A211	**Löschungsfristen**		Mit der Beendigung des Arbeitsverhältnisses.
	A3			**Betroffene Personen**	**Q. 1.23 e 1.31**	**Arbeitnehmer**
	A4			**Datenempfänger**	**Art. 4/9 / Q. 1.34, Q. 1.36 e 1.37**	
Q. 1.34		**A41**		**Datenempfänger 1**		Microsoft
		A42		**Datenempfänger 2**		WOB AG
	A5			**Detaillierte Beschreibung der Datenverabeitung**		
		A51		- Was machen Sie und warum? Unternehmensinformationen werden auf der Verallia Mitarbeiterplattform veröffentlicht und allen Mitarbeitern der Verallia Deutschland AG zur Verfügung gestellt. - Welcher ist der Kontext / Hintergrund? Besserer Informationsaustausch besonders mit Mitarbeiterinnen und Mitarbeitern ohne Verallia-Mailadresse. - Wer ist der zuständige Verantwortliche? Elisa Sauter und Cornelia Banzhaf - Wie üben Sie Ihre Tätigkeit aus? Unternehmenskommunikation und Nachhaltigkeit - Welche Ressourcen werden verwendet? Pimcore (Content Management System) und Evalanche (Datenverwaltungssystem) (Q1.2)		
		A52		Was sind die Vorteile dieser Aktivität / dieses Verarbeitungsvorgangs? - Zugang zu Ressourcen; - Kommunikation; - Informationssicherheit; - Weiterbildung. (Q. 1.27) Wer profitiert von dieser Aktivität / von diesem Verarbeitungsvorgang? - Die Organisation / Firma selbst; - Betroffene Personen. (Q. 1.28)		
		A53		Kann die Aktivität oder ein möglicher Verstoß gegen personenbezogene Daten den betroffenen Personen einen der folgenden Schäden zufügen? - Identitätsdiebstahl; (Q. 1.29)		

DATENSCHUTZ-FOLGENABSCHÄTZUNG			
Projekt (Datenverarubeitung)	Mitarbeiter Portal	**Verantwortliche Stelle**	Verallia Deutschland AG
Bericht Nr.	202102	**Datenschutzbeauftragter**	Thomas Emmendörfer
Ausfertigungsdatum	22.07.2021	**Projektverantwortlicher**	Cornelia Banzhaf (PR Manager); Elisa Sauter (Specialist Communication & CSR); Saskia Müller (DPM)
Aktualisiert am	00.00.0000	**Auftragsverarbeiter**	WOB AG und Microsoft

	A6		**Beschreibung der technischen Anforderungen**		
	A61		**Software**	**Q. 4.1**	Microsoft Excel, Pimcore (Content Management System) und Evalanche (Datenverwaltungssystem)
B			**ANGEMESSENHEIT UND PROPORTIONALITÄT DER VERARBEITUNG**	**Art. 35/7/d**	
	B1		**Würden Maßnahmen implementiert um eine DSGVO konforme Verarbeitung zu versichern?**	**Art. 35/7/d (90)**	
	B11		**Würden Maßnahmen implementiret, welche die Angemessenheit und Proportionalität der Verarbeitung versichern?**		Ja. Daten werden ausschliesslich zum Zugang zum Mitarbeiter Portal verarbeitet. Im Portal werden keine personenbezogenen Daten verarbeitet. ICRF Kontrollmechanismen sind in den Datenverwaltungssystemen implementiert worden.
		B111	**Im Zusammenhang mit dem verfolgten Zweck**	**Art. 5/1/b**	
		B1111	Sind die Zwecke klar beschrieben?		Ja
		B1112	Werden die betroffene Personen ausreichen informiert?	**Q. 2.2**	Benutzer werden darüber informiert, wer ihre Daten sammelt / verwendet.
		B1113	Legitimität der Zwecke	**Q. 2.1; 2.3 e 2.4**	Standardmäßig sind die Datenschutzeinstellungen der Benutzer für diese am günstigsten. Der Zweck jeder Datenverarbeitung wird vor der Erfassung festgelegt. Die Verarbeitungs-, Nutzungs -und Übermittlungsrechten sind eingeschränkt. Die bestehenden Unternehmensrichtlinien minimieren das Risiko vor Hacker-Angriffen.
		B112	**Notwendigkeit der Verarbeitung**	**Art. 5/1/c; Q. 1.26**	
		B1121	Wie notwendig ist diese Aktivität / Verarbeitungsvorgang in Bezug auf ihren Zweck?		Hoch
		B1122	Sind die kategorien personenbezogener Daten adäquat um die festgelegten Ziele zu erreichen?		Ja die Daten sind adäquat um den Zugang zur Plattform zu gewährleisten.
		B1123	Relevanz der Daten		Ja
		B1124	Werden die Daten auf das unbedingt notwendige minimisiert?	**Q. 1.26; 2.6**	Es werden nicht mehr Daten gesammelt, als zur Erreichung eines festgelegten Zwecks erforderlich ist.
		B1125	Sind die Aufbewahrungsfristen festgelegt?	**Art. 5/1/e / Q. 2.10**	Mit Austritt aus dem Unternehmen bzw. Ende der Betriebszugehörigkeit werden die Daten gelöscht.
	B12		**Rechtsmässigkeit der Verarbeitung**	**Art.6 / Q.1.12**	
		B121	Die Verarbeitung ist notwendig für die Konkretisierung eines Vertrages	**Art. 6/1/b**	Die Datenverarbeitung ist notwendig um Mitarbeiter über die Pflichten des Arbeitsverhältnisses zu informieren. Es wird als Kommunikationsmittel zwischen Verallia und Mitarbeiter benutzt
	B2		**Rechte der betroffenen Personen**		
	B21		Informationspflicht - Recht auf Auskunft zu personenbezogenen Daten	**Art. 12, 13 e 14 / Q. 2.11; 2.12; 2.13; 3.1**	Mit der Nutzung der Mitarbeiter Portal sollte eine Datenschutzerklärung akzeptiert werden. Benutzer haben die Möglichkeit über info.deutschland@verallia.com Probleme, Bedenken oder Zweifel zu melden.
	B22		Recht auf Auskunftserteilung und auf Datenübertragbarkeit	**Art. 15, 20 / Q. 3.2 e 3.6**	Ja. Es gibt Mechanismen, mit denen betroffene Personen den Zugriff auf die über sie verarbeiteten personenbezogenen Daten anfordern können. Es gibt die Möglichkeit, personenbezogene Daten an die betroffene Person zu übertragen. Benutzer haben die Möglichkeit über info.deutschland@verallia.com Probleme, Bedenken oder Zweifel zu melden.
	B23		Recht auf Berichtigung und Recht auf Datenlöschung ("Recht auf Vergessenwerden")	**Art. 16, 17 e 19 /Q. 2.7; 2.8; 3.3; 3.4.**	Ja
	B24		Widerspruchsrecht	**Art. 18, 19 e 21 /Q. 3.7**	Benutzer haben die Möglichkeit über info.deutschland@verallia.com Probleme, Bedenken oder Zweifel zu melden.
	B25		Beziehungen mit Auftragsverarbeiter	**Art.28**	Ja mit WOB AG (Anhang 1) und Microsoft

verallia

Pr. 59
Plus Privacy Data Protection

			Vor Implementierung der Massnahmen			Nach Implementierung der Massnahmen			Massnahmen zur Risikominimierung														
Projekt	Cod	Risiko	Wahrscheinlichkeit	Schwere	Wert	Wahrscheinlichkeit	Schwere	Wert	a) - i.	a) - ii.	a) - iii.	a) - iv.	a) - v.	a) - vi.	a) - vii.	b) - i.	b) - ii.	b) - iii.	b) - iv.	c) - i.	d) - i.	e) - i.
Mitarbeiter Portal	B21	Nicht ausreichende Information an betroffene Personen	4 - Sehr Hoch	2 - Mittel	8	1 - Reduziert	1 - Reduziert	1	X													
Mitarbeiter Portal	B1122	Exzessive Verarbeitung	2 - Mittel	1 - Reduziert	1	1 - Reduziert	1 - Reduziert	1		X												
Mitarbeiter Portal	A51	Unvollständiges Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO	3 - Hoch	3 - Hoch	9	1 - Reduziert	1 - Reduziert	1			X											
Mitarbeiter Portal	B26	Risiko der Nutzung eines Auftragsverarbeiters ohne Vertrag nach Art. 28 DSGVO	3 - Hoch	3 - Hoch	9	1 - Reduziert	1 - Reduziert	1				X										
Mitarbeiter Portal	C121	Unbefugten Zugriff	3 - Hoch	2 - Mittel	6	1 - Reduziert	1 - Reduziert	1					X									

Maßnahme zur Risikominimierung

Maßnahme zur Risikominimierung	Cod. Maßnahme	Beschreibung
Datenschutzerklärung - Art 13 DSGVO	i. a) i.	Datenschutzerklärung nach Art. 13 DSGVO bei "erstlogin" mit Beschreibung der Verarbeitung, Rechte der Betroffene Personen und Kontakt der Verantwortlichen Stelle sowie Datenschutzbeauftragters. Link zur Datenschutzerklärung sowie Datenschutzerklärung für Verallia Mitarbeiter: " Bitte behandeln Sie Ihre Zugangsdaten vertraulich. Ihre Daten werden von der Verallia Deutschland AG, mit Sitz in Oberlandstrasse 88410 Bad Wurzach, Deutschland verarbeitet mit dem Zweck des Zugriffs der Mitarbeiter auf das Mitarbeiter Portal der Vitallia. Ihre Daten werden zur Erfüllung des Arbeitsvertrages zwischen dem Mitarbeiter und Verallia verarbeitet und ausschliesslich für oben genannten Zweck benutzt. Die betroffene Person hat gemäß und vorbehaltlich der Voraussetzungen der anwendbaren Datenschutzgesetze, denen diese Erklärung unterliegt, folgende Rechte: i)Recht auf Auskunft über die Erhebung und Nutzung personenbezogener Daten ii)Recht auf Zugang zu und Erhalt einer Kopie der personenbezogenen Daten, die Verallia von der betroffenen Person besitzt iii)Recht auf Berichtigung, falls personenbezogene Daten, die Verallia von der betroffenen Person besitzt, unzutreffend oder unvollständig sind iv)Recht auf Vergessen, d. h. Recht,, sämtliche personenbezogenen Daten, die Verallia von der betroffenen Person besitzt, zu löschen und früher zu löschen als oben festgelegt v)Recht auf Einschränkung (d. h. Verhinderung) der Verarbeitung personenbezogener Daten vi)Recht auf Datenübertragung (d. h. Recht auf Erhalt einer Kopie der personenbezogenen Daten zur Nutzung bei anderen Dienstleistungserbringern oder Organisationen) viii)Recht, der Verallia die Nutzung personenbezogener Daten für bestimmte Zwecke zu untersagen ix)Rechte in Bezug auf automatisierte Entscheidung und Profilerstellung x)Recht, eine Einwilligungserklärung jederzeit zu widerrufen. Sollten sie Fragen über Ihre Datenschutzrechte haben, können sie siech jederzeit an den Datenschutzbeauftragten Thomas Emmendörfer durch die E-mail Adresse info.deutschland@verallia.com wenden. Für weitere Informationen besuchen sie hier die Datenschutzerklärung von Verallia und hier die Datenschutzrichtlinie für Mitarbeiter." (Anhang 2)
Datenminimierung - Art. 5 1 c) DSGVO	ii. a) ii.	Versichern das nur die unbedingt notwendige Daten zum Log-in benutzt werden. Bei erst Log-in E-mail Address und Personalnr. Nach der Erstregistrierung sollte eventuell entweder E-mail oder Personalnummer im Zusammenhang mit Passwort oder MOS Authenticator benutzt werden.
Dokumentation im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO	iii. a) iii.	Die Datenverarbeitung sollte in Verallia's Muster Verzeichnis der Verarbeitungstätigkeiten dokumentiert werden.
Auftragsverarbeitungsvertrag nach Art. 28 DSGVO	v. a) iv.	Muster Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO zwischen Verallia Deutschland AG und WOB AG entspricht die Voraussetzungen von Art. 28 DSGVO. A Anlage 2 - Liste der bestehenden Subuntrenehmer zum Zeitpunkt des Vertragsschlusses soll kontrolliert werden, insbesondere "LinkedIn" und "Instagram". Bei diesen Unterauftragsverarbeiter handelt es sich um sozialen Netwerken welche Daten eventuell veröffentlichen könnten. Es sollen Auftragsverarbeitungsverträge mit allen Auftragsverarbeiter absgeschlossen werden, inklusive im Falle einer Datenverarbeitung, Pimcore (Content Management System), Evalanche (Datenverwaltungssystem) und Microsoft.
Benutzung des Protokolls "https://".	vi. a) v.	Verallia soll die Benutzung des Protokolls "https://" bevorzügen um dem Schutz vor unbefugtem Zugriff zu gewährleisten.

Risikostufen

Wahrscheinlichkeit	Schwere
1 - Reduziert	1 - Reduziert
2 - Mittel	2 - Mittel
3 - Hoch	3 - Hoch
4 - Sehr Hoch	4 - Sehr Hoch

Wahrscheinlichkeit	Schwere			+
	4	3	2	1
Sehr Hoch	16	12	8	4
Hoch	12	9	6	3
Mittel	8	6	4	2

Die Verarbeitung wird nach Implementierung der vorgeschlagenen Massnahmen vom Datenschutzbeauftratgter genehmigt.

Projektverantwortlicher **Datenschutzbeauftragter** **DPM**

ANHANG 1

Vereinbarung zur Auftragsverarbeitung (AV) gemäß Art. 28 DSGVO

zwischen

Verallia Deutschland AG
Oberlandstraße
88410 Bad Wurzach
Deutschland

nachstehend **„Verantwortlicher“**

und

wob AG
Werner-Heisenberg-Straße 8-10
68519 Viernheim
Deutschland

nachstehend **“Auftragsverarbeiter“**

schließen folgenden Vertrag:

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind lautet wie folgt:

Der Auftraggeber unterliegt folgenden besonderen Geheimnisschutzregeln, die auch vom Auftragsverarbeiter zu beachten sind: Keine

Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:
[Hier müssen sämtliche Leistungen im Rahmen der Verarbeitung personenbezogener Daten benannt werden.]

Kampagnen Management, ggf. Sichtung und Optimierungen des Analytics-Accounts, ggf. Einrichtung von Conversion- & Event-Trackings, ggf. in späteren Projekten.

Verknüpfen von Daten, Zugang zu bestehender CRM- oder Website/E-Mail-Automation-Infrastruktur für Datensichtung (insbesondere Mitarbeiter-Daten), Umsetzung von Kampagnen oder aber auch um ein Scoring Modell aufzusetzen/zu optimieren oder ein Nurturing-Programm auf/aus-zubauen.

Außerdem kann es ggf. zu einem späteren Zeitpunkt zu einer Datenverarbeitung im Rahmen etwaiger Social Media-Kampagnen (z.B. über Xing, LinkedIn, o.ä.) kommen. Hierzu würde eine Kontaktliste über die Social Media-Kanäle dem Auftragsverarbeiter (wob) zugänglich gemacht.

Ebenso kann dies eventuell auch Projekte im Rahmen von klassischen (personalisierten) Werbemitteln (Mailings, etc.) betreffen.

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:
[Hier muss eine detaillierte Aufstellung der verarbeiteten Datenarten erfolgen (z.B.: Daten von Bürgern, Name, Vorname, Anschrift Geburtsdatum, Beruf, etc.)]

- Personenstammdaten (Anrede, Titel, Vorname, Nachname, Position, Firma, Website der Firma, E-Mail-Adresse, Telefonnummer, Adresse, Opt-In-Status, Rolle.

- Kommunikationsdaten (E-Mail-Adresse, Opt-In/Opt-Out für E-Mail-Kommunikation)

- Mitarbeiter-Daten (Personalnummer)

- Verhaltensdaten (E-Mail-Öffnungen, Klicks, Downloads, etc.)

- ggf. Interessenten und Produktinformationen

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

Kategorien:
[Auflistung der betroffenen Personengruppen; vorliegend z.B. Mitarbeiter, Kunden, etc.]

- Leads (Interessenten/potenzielle Kunden)
- (Bestands-) Kunden
- Händler
- Mitarbeiter
- Lieferanten

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:
[Detaillierte Beschreibung der Übermittlungswege]

Personenbezogene Daten werden entweder physisch auf einem Datenträger oder über einen sicheren, verschlüsselten Weg übermittelt (individuell freigegebener Ordner in OneDrive von Office 365).
Zugriff auf Lead- und Kundenstammdaten über einen persönlichen evalanche-/CRM-Zugang.

Ggf. Social Media-Kanäle, wie etwa Xing oder LinkedIn:
Die Daten werden im Agency Account der Plattform www.xing.com/xam in einer Excel-Tabelle gespeichert. Die Excel-Tabelle kann nach Login in den Agency Account und bei Zugriff auf den Kunden-Account heruntergeladen werden.

LinkedIn: Die Daten werden über eine verschlüsselte Excel-Tabelle per E-Mail für den Auftragsverarbeiter zugänglich gemacht.

1.2 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

1.3 Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

1.4 Die Vergütung wird außerhalb dieses Vertrags vereinbart.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zulassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3 Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen zu implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.

5.3 Sofern der Auftragsverarbeiter nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (hier im Anschluss). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

Silvio Lackner
advertite GmbH
Werner-Heisenberg-Str. 6a
68519 Viernheim
datenschutz@wob.ag

5.4 Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.6 Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in **Anlage 1 (TOM)** dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

6.2 Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

7. Unterstützungspflichten des Auftragsverarbeiters

7.1 Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

7.2 Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragsverarbeiters sind diesem Vertrag abschließend in **Anlage 2 (Sub)** beigefügt. Für die in **Anlage 2 (Sub)** aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.

8.2 Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

8.3 Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können. Der Auftragsverarbeiter ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragsverarbeiters einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.

8.4 Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. Dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.

8.5 Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO ggü. den ihm unterstellten Personen erfüllt hat.

8.6 Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

8.7 Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.

8.8 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragsverarbeiters

9.1 Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.2 Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.

9.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

9.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.

11.2 Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

11.3 Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)

Anlagenverzeichnis

Anlage 1 Technische und organisatorische Maßnahmen (TOM) des Auftragsverarbeiters zur Gewährleistung der Sicherheit der Datenverarbeitung

Anlage 2 Unterauftragsverhältnisse gemäß 8.1 der Auftragsdatenverarbeitung (Sub)

Direkt im Dokument angefügt.

Anlage 1 (TOM) - Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. **Zweckbindung und Trennbarkeit**
Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Logische Mandantentrennung (softwareseitig)
- ☒ Berechtigungskonzept
- ☒ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☒ Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System
- ☒ Trennung von Produktiv- und Testsystem
- ☒ Sonstige:

Die obigen Vorkehrungen zur Zweckbindung und Trennbarkeit gelten nur für den Fall, sofern Daten lokal im Firmengebäude (lokales RZ) gespeichert und verarbeitet werden.

Personenbezogene Daten werden in der Microsoft Cloud gespeichert und verarbeitet und unterliegen hier den Trust Center Vereinbarungen von Microsoft und gemäß den gesetzlichen Bestimmungen nach DSGVO / GoBD.

Personenbezogene Daten im Bereich von Hosting (OVH oder MS-Azure) werden nur dann gespeichert und verarbeitet sofern dies zum Betrieb der Umgebung benötigt wird. Die Zutrittskontrollen entsprechen hier den TOM bzw. Zertifizierungen unserer Subunternehmer.

II. **Vertraulichkeit und Integrität**
Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der

Systeme des Auftragsverarbeiters:
1. Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

AES-Verschlüsselung 256 Bit

2. Pseudonymisierung
„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

- ☒ Nein
- ☐ Ja, und zwar in folgender Art und Weise:

3. Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern (**Zutrittskontrolle**)**:**

☐ Schließsystem mit Codesperre
☒ Manuelles Schließsystem
☐ Biometrische Zugangssperren (Büro und Serverräume)
☒ Sicherheitsschlösser
☒ Schlüsselregelung (Schlüsselausgabe etc.)
☐ Personenkontrolle beim Pförtner / Empfang
☒ Sorgfältige Auswahl von Reinigungspersonal
☒ Sorgfältige Auswahl von Wachpersonal
☒ Zutrittskonzept / Besucherregelung – es werden generell keine Besucher in die IT-Räume ohne Begleitpersonal zugelassen.
☒ Sonstige:

Die obigen Zutrittskontrollen gelten nur für den Fall, sofern Daten lokal im Firmengebäude (lokales RZ) gespeichert und verarbeitet werden.

Personenbezogene Daten werden in der Microsoft Cloud gespeichert und verarbeitet und unterliegen hier den Trust Center Vereinbarungen von Microsoft und gemäß den gesetzlichen Bestimmungen nach DSGVO / GoBD.

Personenbezogene Daten im Bereich von Hosting (OVH oder MS-Azure) werden nur dann gespeichert und verarbeitet sofern dies zum Betrieb der Umgebung benötigt wird. Die Zutrittskontrollen entsprechen hier den TOM bzw. Zertifizierungen unserer Subunternehmer.

4. Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern (**Zugangskontrolle**):

☒ Zuordnung von Benutzerrechten
☒ Erstellen von Benutzerprofilen
☒ Passwortvergabe
☒ Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
☐ Authentifikation mit biometrischen Verfahren (bei Mobile Devices & Desktopsystemen)
☒ Authentifikation mit Benutzername / Passwort / Zertifikaten und 2FA
☒ Zuordnung von Benutzerprofilen zu IT-Systemen über Azure AD
☒ Einsatz von VPN-Technologie (OpenVPN) oder SSL Standards bei der Übertragung von Daten
☒ Verschlüsselung der Datensicherungssysteme (Veeam)
☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
☒ Einsatz von Anti-Viren-Software
☐ Verschlüsselung von Datenträgern in Notebooks
☒ Einsatz einer Hardware-Firewall (OnPremise & Hostingumgebungen bei OVH)
☐ Einsatz einer Software-Firewall in Notesbooks
☒ Sonstige:

Die obigen Zugangskontrollen gelten nur für den Fall, sofern Daten lokal im Firmengebäude (lokales RZ) gespeichert und verarbeitet werden.

Personenbezogene Daten werden in der Microsoft Cloud gespeichert und verarbeitet und unterliegen hier den Trust Center Vereinbarungen von Microsoft und gemäß den gesetzlichen Bestimmungen nach DSGVO / GoBD.

Personenbezogene Daten im Bereich von Hosting (OVH oder MS-Azure) werden nur dann gespeichert und verarbeitet sofern dies zum Betrieb der Umgebung benötigt wird. Die Zugangskontrollen entsprechen hier immer den Vorgaben unserer Subunternehmer. In jedem Fall werden dabei mindestens Benutzername, Passwort und eine 2FA verwendet.

5. Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle):**

☒ Berechtigungskonzept
☒ Verwaltung der Rechte durch Systemadministrator
☒ regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
☒ Anzahl der Administratoren ist das „Notwendigste“ reduziert
☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
☒ Sonstige:

Personenbezogene Daten werden in der Microsoft Cloud gespeichert und verarbeitet und unterliegen hier den Trust Center Vereinbarungen von Microsoft und gemäß den gesetzlichen Bestimmungen nach DSGVO / GoBD.

Personenbezogene Daten im Bereich von Hosting (OVH oder MS-Azure) werden nur dann gespeichert und verarbeitet sofern dies zum Betrieb der Umgebung benötigt wird. Die Zugangskontrollen entsprechen hier immer den Vorgaben unserer Subunternehmer. In jedem Fall werden dabei mindestens Benutzername, Passwort und eine 2FA verwendet.

6. Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle).**

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☒ Sonstige:

Die obigen Eingabekontrollen gelten nur für den Fall, sofern Daten lokal im Firmengebäude (lokales RZ) gespeichert und verarbeitet werden.

Personenbezogene Daten werden nur in der Microsoft Cloud gespeichert und verarbeitet und unterliegen hier den Office 365 Trust Center Vereinbarungen von Microsoft und je nach Schutz und Sicherheitsanforderungen gemäß den gesetzlichen Bestimmungen nach DSGVO / GoBD.

7. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle).**

☒ Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
☐ vorherige Prüfung der und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
☒ schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)

☐ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
☒ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt – sofern nötig
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
☐ laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten
☐ Sonstige:

8. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (**Transport- bzw. Weitergabekontrolle**):

☐ Einsatz von VPN-Tunneln
☒ Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des EMail-Verkehrs)
☒ Verschlüsselung physischer Datenträger bei Transport
☒ Sonstige:

Personenbezogene Daten werden nur in der Microsoft Cloud gespeichert und verarbeitet und unterliegen hier den Office 365 Trust Center Vereinbarungen von Microsoft und je nach Schutz und Sicherheitsanforderungen gemäß den gesetzlichen Bestimmungen nach DSGVO / GoBD. Die Daten werden unter ein Sharepointverzeichnis verschlüsselt, per Zugriffrollenvergabe und Username, Passwort und 2FA ausgetauscht und ggf. dort verarbeitet. Darin enthalten sind die Protokollierung, Sicherung, Versionierung und sichere Löschung bei Abschluss der Verarbeitung.

II. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

☒ Unterbrechungsfreie Stromversorgung (USV)
☒ Klimatisierung der Serverräume
☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
☒ Schutzsteckdosenleisten in Serverräumen
☒ Feuer- und Rauchmeldeanlagen in Serverräumen
☒ Feuerlöschgeräte in Serverräumen
☒ Erstellen eines Backup- & Recoverykonzepts
☒ Testen von Datenwiederherstellung
☒ Notfallpläne
☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
☒ Serverräume nicht unter sanitären Anlagen
☐ belastbares Datensicherungs- und Widerherstellungskonzept vorhanden

III. Besondere Datenschutzmaßnahmen

Es liegen schriftlich vor:

- ☒ interne Verhaltensregeln
- ☐ Risikoanalyse
- ☐ Datenschutz-Folgenabschätzung
- ☐ Datensicherheitskonzept
- ☒ Wiederanlaufkonzept
- ☒ Zertifikat: Siehe Hosting Subunternehmer

- ☐ Sonstiges

IV. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen anlassbezogen prüfen, evaluieren und bei Bedarf anpassen.

Anlage 2 (Sub) – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	Beschreibung der Leistung	Ort der Leistungserbringung
SC Networks GmbH Würmstraße 4 82319 Starnberg https://www.sc-networks.com/legal-notice/	Software „evalanche“ zum Mailversand und Datenerhebung über Formulare	Deutschland
advertite GmbH Werner-Heisenberg-Str. 6a 68519 Viernheim Fon: +49 6204 970 500 https://www.advertite.de/	Support/ Datenschutz/ interne IT-Verwaltung / Software und Development-Mitarbeit	Deutschland
Microsoft Ireland Operations Limited The Atrium Building Block B, Carmanhall Road Sandyford Business Estate Dublin 18 http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=12188	Hosting / Rechenzentrum / SaaS Produkte / Office 365 / MS Azure	Irland
New Work SE Dammtorstraße 30 20354 Hamburg Deutschland Anja Engler Betriebliche Datenschutzbeauftragte Tel.: +49 40 419 131-0 Fax: +49 40 419 131-11 E-Mail: info@xing.com E-Mail: Datenschutzbeauftragter@xing.com	Internetdienstleistungen / Werbeplattform / Ad Server Soziales Netzwerk / Leadgenerierung	Deutschland
LinkedIn Ireland Unlimited Company Wilton Place Dublin 2, Ireland https://www.linkedin.com/legal/impressum	Internetdienstleistungen / Werbeplattform / Ad Server Soziales Netzwerk / Leadgenerierung	Deutschland
Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Ireland https://help.instagram.com/	Internetdienstleistungen / Werbeplattform / Ad Server Soziales Netzwerk / Leadgenerierung	Deutschland
OVH GmbH Datenschutzbeauftragter: Dr. Sebastian Kraska Dudweiler Landstraße 5 66123 Saarbrücken E-Mail: datenschutz@ovh.de https://www.ovh.de/unternehmen/datenschutz.xml	Hosting / Rechenzentrum / ASP	Frankreich / Deutschland

ANHANG 2

DATENSCHUTZRICHTLINIE FÜR MITARBEITER

VERALLIA respektiert die Privatsphäre aller seiner Mitarbeiter und garantiert die verantwortungsvolle Verarbeitung ihrer personenbezogenen Daten in Übereinstimmung mit den geltenden Rechtsvorschriften, und unter vollständiger Achtung/Wahrung der geltenden europäischen und nationalen Datenschutzgesetze.
Aus Gründen des Vertrauens, der Einfachheit und der Transparenz verpflichtet diese Datenschutzrichtlinie VERALLIA, die Bestimmungen dieses Dokuments einzuhalten.

EINLEITUNG

Für VERALLIA hat der Schutz personenbezogener Daten höchste Priorität.
In dieser Datenschutzrichtlinie für Mitarbeiter wird erläutert, wie VERALLIA die personenbezogenen Daten seiner Mitarbeiter schützt.
Die Mitarbeiter behalten sämtliche/ alle verfügbaren Rechte gemäß den geltenden Gesetzen. Diese Richtlinie wird nur dann angewendet, wenn diese einen zusätzlichen Schutz für Mitarbeiterdaten/ personenbezogene Daten der Mitarbeiter darstellt/bietet. Wenn das geltende allgemeine Recht in Bezug auf den Schutz günstiger ist, sollte dieses (Recht) angewendet werden.
Der Schutz personenbezogener Daten liegt in der Verantwortung unserer Organisation. Daher verpflichten wir uns, diese Richtlinie zu aktualisieren, sobald neue Gesetze und / oder neue Datenverarbeitungspraktiken eingeführt werden.

DPO

VERALLIA hat einen Datenschutzbeauftragten (DPO) ernannt, der zur Klärung aller Fragen im Zusammenhang mit den Datenschutzrichtlinien und -praktiken des Unternehmens zur Verfügung steht. Der Name und die Kontaktdaten des Datenschutzbeauftragten lauten wie folgt:

Thomas Emmedörfer
Oberlandstraße 1-8 88410 Bad Wurzach
thomas.emmendoerfer@verallia.com/info.deutschland@verallia.com

SAMMELN UND VERARBEITEN VON PERSONENBEZOGENEN DATEN

Verallia sammelt Informationen über seine Mitarbeiter ODER Verallia sammelt und verarbeitet personenbezogene Daten seiner Mitarbeiter. Diese Mitarbeiterdaten werden von Verallia nur an Dritte oder Subunternehmer weitergegeben, die die Einhaltung der geltenden Datenschutzvorschriften gewährleisten ODER die die Einhaltung der Datenschutzgesetze (Datenschutzrichtlinien) garantieren.

1. Was wir mit den von Ihnen angegebenen personenbezogenen Daten machen:

Die Übermittlung / Mitteilung personenbezogener Daten ist eine notwendige Voraussetzung für den Abschluss eines Arbeitsvertrages. Ohne diese Daten wäre Verallia nicht in der Lage seinen gesetzlichen Verpflichtungen als Arbeitgeber nachzukommen oder mit seinen Arbeitnehmern zu kommunizieren.

Zu diesem Zweck werden personenbezogene Daten wie Name, persönliche Adresse, Personalnummer, Steuer-Identifikationsnummer, Telefonnummer, E-Mail-Adresse, Bankverbindung u.a. verarbeitet. Der Name, das Bild und die Funktion der Mitarbeiter können im sozialen Netzwerk LinkedIn® sowie auf internen Websites (z. B. Intranet, SharePoint usw.) zur Verfügung gestellt werden / zugänglich gemacht werden.

Um den gesetzlichen Verpflichtungen nachzukommen / Um die Einhaltung gesetzlicher Verpflichtungen zu gewährleisten, können personenbezogene Daten der Mitarbeiter an externe Stellen (sonstige Stellen, Dienstleister, Gerichte und Behörden) weitergeleitet werden, die Aufgaben im Zusammenhang mit dem Arbeitsrecht, dem Lohnsteuerecht, der medizinischen oder der Gesundheitsversorgung oder des Sozialversicherungsrechts wahrnehmen. Wie auch/Sowie auch an andere Behörden und Stellen der öffentlichen Verwaltung (Arbeitsschutzbehörden; Finanzämter; Integrationsämter) oder Krankenkassen und private Krankenversicherungen, Träger der gesetzlichen Rentenversicherung, Träger der gesetzlichen Pflegeversicherung, Träger der gesetzlichen Unfallversicherung. Personenbezogene Daten können auch an andere Unternehmen weitergeleitet/übermittelt werden, wenn und soweit diese sich im Rahmen der Tätigkeiten einer Niederlassung befinden oder in ähnlichen Fällen, die in einem Tarifvertrag festgelegt sind.

Die Daten des Arbeitnehmers werden so lange aufbewahrt, wie der Arbeitsvertrag in Kraft ist und bis (.) Jahre nach Vertragsende und danach, wenn ein laufendes Rechts- oder Verwaltungsverfahren vorliegt, in dem die personenbezogenen Daten möglicherweise verwendet werden oder wenn diese gesetzlich aufbewahrt werden müssen. Personenbezogene Daten für Steuerzwecke können je nach Einzelfall 6 bis 10 Jahre aufbewahrt werden. Bei gesundheitsbezogenen Daten im Bereich Gesundheit und Sicherheit am Arbeitsplatz werden die Daten bis zu (.) Jahre aufbewahrt.

Alle Mitarbeiter haben ein grundsätzliches Recht auf Auskunft über die beim Arbeitgeber gespeicherten Daten zu seiner Person und können über die Personalabteilung Zugang zu diesen anfordern. Wenn Sie ein Mitarbeiter von Verallia sind und Zugriff auf Ihre personenbezogenen Daten benötigen, wenden Sie sich bitte an info.deutschland@verallia.com.

2. Verarbeitung personenbezogener Daten – Primärnutzung / Primäre Zweck der Datenverarbeitung

a) Personalwesen: Was beinhaltet dieser Zweck? Wir verarbeiten Ihre personenbezogenen Daten für die Einstellung, den Abschluss und die Ausführung des Arbeitsvertrags oder eines anderen Vertrags mit dem Arbeitnehmer sowie für die Arbeitsorganisation ODER die Organisation der täglichen Arbeit erforderlich wie z.B für Arbeitsplatzverlagerungen, Vergütungen und Leistungen, Zahlungen, steuerrechtliche Angelegenheiten, Karriere- und Talentförderung, Leistungsbewertungen, Schulungen, Urlaubsplanung, Reisen, Ausgaben und Kommunikation.

b) Ausführung von Geschäftsprozessen und internes Management: Personenbezogene Daten werden für die Ausübung und Organisation des Geschäftsbetriebs verarbeitet. Diese Verarbeitung personenbezogene Daten umfasst Aktivitäten wie Planung und Arbeitszeiten, Kontrolle der Arbeitszeiten bzw. Arbeitszeiterfassung, Anwesenheitskontrolle, Verwaltung des Unternehmensvermögens, Bereitstellung von IT-Diensten, Audits, professionelle Kontrollen, Management und Verwendung/Nutzung von Mitarbeiterdatenbanken.

c) Gesundheit und Sicherheit am Arbeitsplatz: Die(se) Verarbeitung umfasst alle Verarbeitungstätigkeiten, die für Sicherheit und Gesundheit am Arbeitsplatz, den Schutz

der Mitarbeiter und der Vermögenswerte von Verallia, sowie für die Verwaltung und Zugangskontrollen zu Einrichtungen erforderlich sind.

d) Bewertung/Evaluierung und Entwicklung: diese Verarbeitung umfasst Aktivitäten wie die Durchführung von Fragebögen für Mitarbeiter und/oder die Verwaltung von Fusionen und Übernahmen.

e) Erfüllung rechtlicher Verpflichtungen: diese Verarbeitung umfasst die Erfüllung aller gesetzlichen Verpflichtungen, denen Verallia unterliegt, wie z. B. die Verwaltung/Regelung von Meldelinien für Whistleblowing/ Meldewege für Whistleblowing.

f) Schutz vitaler Interessen der Beschäftigten / Schutz der vitalen Interessen der Mitarbeiter: Der Zweck, für die die personenbezogenen Daten verarbeitet werden, umfasst den Schutz der vitalen Interessen der Mitarbeiter im Bedarfsfall.

Sollten irgendwelche Zweifel an der Rechtmäßigkeit der Verarbeitung personenbezogener Arbeitnehmerdaten für die oben aufgeführten Beispiele bestehen, sollte vor jeder Erhebung der Datenschutzbeauftragte um Rat gefragt werden.

3. Zustimmung/ Einwilligung

Wenn keiner der oben genannten Gründe zutrifft, kann Verallia die Zustimmung des Mitarbeiters zur Verarbeitung Ihrer personenbezogenen Daten anfordern. Der Antrag auf Zustimmung bedarf der vorherigen Genehmigung durch den Datenschutzbeauftragten.
Jeder Mitarbeiter kann seine Einwilligung jederzeit ohne Konsequenzen für sein Arbeitsverhältnis verweigern oder widerrufen/ zurückzuziehen. Der Widerruf der Einwilligung beeinträchtigt nicht die Rechtmäßigkeit der Verarbeitung, für die sie erteilt wurde ODER Der Widerruf der Einwilligung beeinträchtigt nicht die Rechtmäßigkeit der auf der Grundlage der zuvor erteilten Einwilligung durchgeführten Behandlung.

4. Verarbeitung personenbezogener Daten – Sekundärnutzung ODER Datenverarbeitung für sekundäre Zwecke

Im Allgemeinen sollten personenbezogene Mitarbeiterdaten nur für die primären Zwecke verarbeitet werden, für die sie ursprünglich erfasst wurden (ursprünglicher Zweck). Mitarbeiterdaten können auch für folgende sekundäre Zwecke (Sekundärnutzung) verarbeitet werden:

a) Übertragen von Daten in eine Datei;
b) interne Audits oder Untersuchungen;
c) Prozessimplementierung/Umsetzung von Prozessen;
d) statistische, historische oder wissenschaftliche Forschung;
e) Vorbereitung oder Mitwirkung an der Beilegung von Streitigkeiten;
f) Juristische oder geschäftliche/kommerzielle Beratung, oder
g) Versicherungsunternehmen / Versicherungen

5. Spezifische Zwecke für die Verarbeitung sensibler Daten

Verarbeitet werden können auch zusätzliche Informationen, die je nach Art und Zweck der Verarbeitung erforderlich sein können, einschließlich sensibler Daten, wie Gesundheitsdaten/ persönliche gesundheitsbezogene Daten, wenn beispielsweise ein Sicherheits- und Gesundheitsdienst, eine Mahlzeit mit einer bestimmten Diät oder wenn im Krankheitsfall Unterstützung bereitgestellt wird.

Sensible Daten sind personenbezogene Daten von Mitarbeitern, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben (und der sexuellen Orientierung), sowie Daten über strafrechtliche Verurteilungen, Straftaten, Vorstrafen und andere Verstöße.

Verallia verarbeitet sensible personenbezogene Daten nur dann, wenn dies für die rechtmäßige Verarbeitung im Beschäftigungskontext erforderlich ist.
Die folgenden Kategorien sensibler Daten können nur für einen oder mehrere der unten angegebenen Zwecke verarbeitet werden:

a) Daten über rassische und ethnische Herkunft: Fotos und Videobilder von Mitarbeitern können als rassische oder ethnische Daten gelten. Verallia kann Fotos und Videobilder zum Schutz der Vermögenswerte von Verallia und seiner Mitarbeitern, für den Zugriff auf die Räumlichkeiten, aus Sicherheitsgründen und zur Aufnahme in die Mitarbeiterdatenbank verarbeiten.

b) Daten zur körperlichen oder geistigen Gesundheit (einschließlich Diagnosen zur körperlichen oder geistigen Gesundheit, sowie Daten zu Behinderungen und Abwesenheiten aufgrund von Krankheit oder Schwangerschaft):

i) Bereitstellung von Gesundheitsdiensten für einen Mitarbeiter, sofern die relevanten Gesundheitsdaten von bzw. unter der Aufsicht eines Angehörigen der Gesundheitsberufe verarbeitet werden, die der beruflichen Vertraulichkeit unterliegen/unterstellt sind;

ii) Renten- und Pensionspläne, Kranken- und Sozialversicherungspläne, Mutterschaftsprogramme, Vaterschafts- oder Familienurlaub, sowie Tarifverträge (oder ähnliche Verträge), aus denen sich Rechte für Arbeitnehmer ergeben;

iii) Wiedereingliederung/Reintegration oder Unterstützung von Arbeitnehmern, die Anspruch auf Leistungen im Zusammenhang mit Krankheit oder Arbeitsunfähigkeit haben;

iv) Bewertung und Entscheidungsfindung über die Aufrechterhaltung oder Eignung für bestimmte Positionen, Projekte oder Verantwortlichkeiten;
v) Bereitstellung von Ausrüstung am Arbeitsplatz zur Anpassung an gesundheitliche Probleme oder Behinderungen.

c) Strafrechtliche Daten (einschließlich Daten zu Straftaten, Vorstrafen, strafrechtlichen Verurteilungen, andere Verstöße):
i) Bewertung bei der Einstellung von Mitarbeitern in Bezug auf einen sensiblen Arbeitsplatz;
ii) Zum Schutz der Interessen von Verallia in Bezug auf Straftaten oder mutmaßliche Straftaten, die gegen Verallia oder seine Mitarbeiter oder innerhalb der Firmeneinrichtungen begangen wurden.

6. Allgemeine Zwecke der Verarbeitung sensibler Daten

Zusätzlich zu den oben aufgeführten spezifischen Zwecken können auch Kategorien sensibler Daten mit folgenden Zwecken verarbeitet werden:

(i) Wie gesetzlich vorgeschrieben oder erlaubt;
(ii) Zur Einleitung oder Verteidigung von (bei) Rechtsstreitigkeiten;
(iii) Zum Schutz der vitalen Interessen der Mitarbeiter;
(iv) Wenn sensible Daten vom Mitarbeiter selbst veröffentlicht wurden / an die Öffentlichkeit bekannt oder zugänglich gemacht wurden.

Jegliche Verarbeitung sensibler Daten aufgrund einer gesetzlichen Anforderung oder der Zustimmung des Mitarbeiters wird zuvor vom Datenschutzbeauftragten analysiert.

KORRESPONDENZ

Jeder Austausch professioneller Korrespondenz, sei es per Post, E-Mail oder anderweitig, kann gespeichert und für folgende Zwecke verwendet werden: Beantwortung, Senden von Korrespondenz zu ähnlichen Themen oder Aufzeichnung zu Protokollierungszwecken. Wenn Sie möchten, dass Verallia Ihre persönlichen Daten löscht oder Ihre Daten nicht mehr zum Senden jeglicher Art von Kommunikation verwendet, wenden Sie sich bitte an den Datenschutzbeauftragten.

INFORMATIONSÜBERMITTLUNG AN DRITTE

Verallia kann auf Anfrage und im gesetzlich zugelassenen Umfang Informationen an Behörden (z.B. Gerichte) weitergeben, um den gesetzlichen Verpflichtungen des Unternehmens nachzukommen.
Verallia kann ebenfalls auf Anfrage und unter Einhaltung der im Datenschutzgesetz vorgeschriebenen Schutzvorkehrungen Informationen in Bezug auf personenbezogene Daten an Vollzugsbeamte, externe Prüfer, Wirtschaftsprüfer, Rechtsanwälte, Schulungs- und Zertifizierungsstellen und andere verbundene Stellen weitergeben.
Vereinzelt kann Verallia beantragen/verlangen, dass Dritte Informationen zu Veranstaltungen weitergeben, an denen Verallia Mitarbeiter teilgenommen haben, sowie zu Produkten oder Dienstleistungen, die sie erworben haben.

In Ausnahmefällen und (nur) zur Verfolgung legitimer Zwecke, wie die Erfüllung eines Vertrages oder rechtlicher Verpflichtungen, oder zum Schutz wesentlicher Interessen der betroffenen Person oder Dritter, kann Verallia andere Informationen auf Anfrage oder mit ausdrücklicher Genehmigung verarbeiten.

DATENÜBERMITTLUNG AN DRITTLÄNDER

Verallia DE ist ein deutsches Unternehmen, das in Deutschland tätig ist. Die gesammelten/erhobenen Informationen werden nicht in Länder außerhalb der Europäischen Union (EU) übertragen. Bei Datenübermittlungen in Länder außerhalb der EU werden Länder vorrangig behandelt, die einer EU-Angemessenheitsentscheidung gemäß Artikel 45 der DSGVO unterliegen.
Sollte dies nicht erfolgen, trifft Verallia die erforderlichen Vorkehrungen, um den Schutz und die Sicherheit Ihrer personenbezogenen Daten gemäß Artikel 46 der DSGVO (Vorliegen geeigneter Garantien) zu gewährleisten und sie nur für die Zwecke zu verwenden, für die sie erhoben wurden, und gemäß den beschriebenen Praktiken in dieser Datenschutzerklärung.

RECHTE DER BETROFFENEN PERSONEN

Um die Verarbeitung personenbezogener Daten transparent und gerecht zu halten, gewährleistet Verallia als Verantwortlicher der Verarbeitung den betroffenen Personen folgende Rechte:

1. Recht auf Auskunft

Das Auskunftsrecht besteht aus dem Recht der betroffenen Person, auf seine von Verallia verarbeiteten personenbezogenen Daten und Informationen zur deren Verarbeitung zuzugreifen. Auf Anfrage kann die betroffene Person Zugang über deren Verarbeitungszwecke, der verarbeiteten Kategorie personenbezogener Daten, dem Empfänger bzw. Kategorien von Empfängern, die geplante Speicherdauer bzw. Kriterien für deren Festlegung, Angaben zu der Herkunft der Daten (falls diese nicht direkt von Verallia erhoben wurden) und gegebenenfalls über das etwaige Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling erhalten.

2. Recht auf Berichtigung

Das Recht auf Berichtigung ist das Recht der betroffenen Person, die unverzügliche Berichtigung unrichtig oder unvollständig verarbeiteter Daten über sich selbst zu verlangen. ODER Das Recht auf Berichtigung ist das Recht der betroffenen Person, Berichtigung personenbezogener Daten zu verlangen, wenn diese falsch, ungenau oder unvollständig sind.

3. Recht auf Datenlöschung ("Recht auf Vergessenwerden")

Als betroffene Person / Als Inhaber personenbezogener Daten kann der Mitarbeiter Verallia auffordern, die Verarbeitung seiner Daten einzustellen oder zu löschen, wenn dies für die Erfüllung seines Arbeitsvertrags nicht erforderlich ist. Der Mitarbeiter kann Verallia auch auffordern, die Verarbeitung seiner personenbezogenen Daten für bestimmte Zwecke einzustellen.

4. Recht auf Einschränkung der Verarbeitung und Widerspruch

Als betroffene Person / Als Inhaber personenbezogener Daten hat der Mitarbeiter das Recht, von Verallia die Einschränkung der Verarbeitung zu verlangen. Er hat außerdem das Recht, der Verarbeitung seiner personenbezogenen Daten zu widersprechen oder seine Einwilligung jederzeit zu widerrufen. Der Widerruf der Einwilligung beeinträchtigt nicht die Rechtmäßigkeit der Verarbeitung, für die sie erteilt wurde ODER Der Widerruf

der Einwilligung beeinträchtigt nicht die Rechtmäßigkeit der auf der Grundlage der zuvor erteilten Einwilligung durchgeführten Behandlung.

5. Beschwerderecht

Als betroffene Person hat der Mitarbeiter das Recht, eine Beschwerde bei der Aufsichtsbehörde einzureichen, wenn er der Ansicht ist, dass seine Rechte als Inhaber personenbezogener Daten verletzt werden.

6. Recht auf Übertragbarkeit / Datenübertragbarkeit

Als betroffene Person / Als Inhaber personenbezogener Daten hat der Mitarbeiter das Recht, seine personenbezogenen Daten [in einem strukturierten, gängigen und maschinenlesbaren Format] zu erhalten und diese an einen anderen Verantwortlichen zu übermitteln.

7. Recht, sich keiner automatisierten Entscheidung einschließlich Profiling zu unterwerfen

Als betroffene Person / Als Inhaber personenbezogener hat der Mitarbeiter das Recht, keiner Entscheidung zu unterliegen, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profilerstellung, beruht.

8. Informationsrecht

Der Mitarbeiter hat ebenfalls das Recht, informiert zu werden, wenn ein Verstoß/eine Verletzung gegen personenbezogene Daten vorliegt, der (die) voraussichtlich zu einem erheblichen Risiko für seine Rechte und Freiheiten führen könnte. Der Mitarbeiter kann sich an den Datenschutzbeauftragten wenden, um herauszufinden, ob seine personenbezogenen Daten von Verallia verarbeitet werden. Die Kontaktdaten des Datenschutzbeauftragten finden Sie auf der ersten Seite dieser Richtlinie.

VERFAHREN ZUR AUSÜBUNG DER RECHTE DER BETROFFENEN PERSON(EN)

Der Mitarbeiter muss seine Anfrage an den Personalleiter senden. Bevor Verallia auf die Anfrage antwortet, kann Verallia vom Mitarbeiter einen Identitätsnachweis und/sowie die Angabe folgender Informationen verlangen:

a) die Art der betreffenden Daten, die zugänglich gemacht werden sollen;
b) auf welchem System diese Daten (möglicherweise) gespeichert sein könnten;
c) die Umstände, unter denen Verallia die Mitarbeiterdaten erhalten hat;

e) Im Falle eines Antrags auf Berichtigung oder Widerspruch, die Gründe warum die personenbezogenen Daten falsch oder unvollständig sind bzw. nicht gesetzeskonform behandelt wurden.

Verallia kann die Anfrage einer betroffenen Person ablehnen, falls:

a) die Anfrage nicht den oben genannten Anforderungen entspricht oder nicht spezifisch genug ist;

b) die Identität des Mitarbeiters nicht nachgewiesen werden kann;

c) das Zeitintervall / die Zeitspanne zwischen mehreren Anfragen derselben betroffenen Person nicht angemessen ist;

Frist zur Beantwortung des Auskunftsbegehrens / Frist für die Beantwortung von Anträgen

Innerhalb eines Monats nach Eingang des Antrags/ Auskunftsbegehrens informiert der Personalmanager oder Datenschutzmanager (DPM) den Mitarbeiter schriftlich a) über die Stellungnahme von Verallia bezüglich des Antrags und alle Maßnahmen, die Verallia ergriffen hat oder ergreifen wird oder (b) über das endgültige Datum, an dem die betroffene Person über die Stellungnahme von Verallia informiert wird.
Der Mitarbeiter kann sich beim Datenschutzbeauftragten beschweren, wenn die Antwort als nicht zufriedenstellend betrachtet wird / sollte die Antwort nicht zufrieden stellend ausfallen.

INFORMATIONSSICHERHEIT

Um den Schutz und Vertraulichkeit der von Verallia verarbeiteten Daten zu gewährleisten, unterhält Verallia Mechanismen für die Sicherheit physischer, digitaler und administrativer Prozesse und bietet seinen Mitarbeitern in diesem Bereich Schulungen an.

Die Sicherheit von (bei) Verallia basiert auf drei Grundprinzipien: Integrität, Vertraulichkeit und Verfügbarkeit.
Verallia hat eine Reihe technischer und organisatorischer Maßnahmen getroffen, um den Schutz der von Verallia verarbeiteten personenbezogenen Daten zu gewährleisten. Verallia hat eine Reihe von Maßnahmen verabschiedet, die spezifisch dokumentiert sind, und an die Verallia Vorgaben gebunden und zu eingehalten werden müssen. Um die Umsetzung dieser Sicherheitsmaßnahmen sicherzustellen, führt Verallia regelmäßige Audits durch.

SCHULUNG / AUSBILDUNG

Verallia schult seine Mitarbeiter durch Sensibilisierungsprogramme, E-Learning-Kurse, Schulungen, Webinare und Workshops über die Bedeutung der vertraulichen Verarbeitung personenbezogener Daten und der Informationssicherheit.

DISZIPLINARMAßNAHMEN

Verallia kann Disziplinarmaßnahmen gegen diejenigen verhängen, die die Datenschutzbestimmungen nicht einhalten.

SPEICHERUNG/LAGERUNG DER INFORMATION

Ihre Personenbezogenen Daten werden nur in der Microsoft Cloud gespeichert und verarbeitet und unterliegen hier den Office 365 Trust Center Vereinbarungen von Microsoft und je nach Schutz und Sicherheitsanforderungen gemäß den gesetzlichen Bestimmungen nach DSGVO/GoBD. Die Daten werden unter ein Sharepointverzeichnis verschlüsselt, per Zugriffrollenvergabe und Username, Passwort und 2FA ausgetauscht und ggf. dort verarbeitet, mit Sitz in der Europäischen Union. Darin enthalten sind die Protokollierung, Sicherung, Versionierung und sichere Löschung bei Abschluss der Verarbeitung.

Verallia speichert Ihre personenbezogenen Daten für die Zeit, die erforderlich ist, um die Zwecke zu erlangen, für die Daten erhoben (und weiterverarbeitet) wurden. Um weitere Informationen darüber zu erhalten, wo und wie lange Ihre personenbezogenen Daten aufbewahrt werden und welche Rechte Sie haben, auf diese zuzugreifen und zu löschen, wenden Sie sich bitte an den Datenschutzbeauftragten. Die Kontakte des Datenschutzbeauftragten befinden sich auf der Startseite dieser Richtlinie.

INFORMATIONSPFLICHT / Worüber muss die betroffene Person informiert werden?

Alle Mitarbeiter haben das Recht, bei der Erhebung ihrer personenbezogenen Daten über eine Reihe grundlegender Informationen informiert zu werden.

Während der Geltungsdauer des Dienstverhältnisses mit Verallia und immer wenn personenbezogene Daten erhoben werden müssen wird der Mitarbeiter, in diesem Sinne, in präziser, transparenter, verständlicher und leicht zugänglicher Form (in einer klaren und einfachen Sprache) über allen von der DSGVO auferlegten Bestimmungen im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten informiert.

ÄNDERUNG UND AKTUALISIERUNG

Die gegenwärtige Fassung ist vom 30.06.2021 datiert.

Bei Verallia arbeiten wir an der kontinuierlichen Verbesserung unserer Prozesse. Das gegenwärtige Dokument kann geändert werden und wir arbeiten an seiner Erweiterung in mehreren Bereichen. Verallia behält sich daher das Recht vor, die Datenschutzrichtlinie für Mitarbeiter jederzeit und aus beliebigen Gründen zu ändern, ohne dass die Inhaber personenbezogener Daten ODER ohne dass die betroffenen Personen, denen die verarbeiteten personenbezogenen Daten gehören, benachrichtigt werden.
Sie können die aktualisierte Datenschutzrichtlinie für Mitarbeiter und / oder eventuelle Änderungen unter folgendem Link einsehen: https://de.verallia.com/s/datenschutz

FRAGEN ODER BESCHWERDEN

Bei Zweifeln/Fragen, Bedenken oder Beschwerden im Zusammenhang mit der Verarbeitung personenbezogener Daten wenden Sie sich bitte per E-Mail an den Datenschutzbeauftragten:
Thomas Emmendörfer
info.deutschland@verallia.com

ANHANG 3

Verallia DE

Datenschutz-Folgenabschätzung

Herzlich Willkommen und vielen Dank für Ihre Teilnahme **am Fragebogen zur Umsetzung der Datenschutzfolgenabschätzung**, durch den das neue Projekt Ihres Unternehmens dem Verallia DE - Datenschutzteam vorgestellt werden soll!

Unser erklärtes Ziel ist es, den Erfolg Ihres Projektes zu maximieren, ohne den Schutz der darin behandelten personenbezogenen Daten zu vernachlässigen, um alle Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 - der Datenschutz-Grundverordnung (fortan DSGVO) einzuhalten.

Der Datenschutzmanager (DPM) nimmt durch diesen Fragebogen Kenntnis über das betreffende Projekt, sowie der darin behandelten personenbezogenen Daten. Dies ermöglicht dem DPM die Erstellung von Vorgaben und Leitlinien für Ihr Unternehmen, die für die Erfüllung der DSGVO unerlässlich sind.

Nach Artikel 35 der DSGVO ist Verallia verpflichtet, Datenschutzfolgenabschätzung (DSFAs) durchzuführen.

Diese DSFA wird dem Datenschutzbeauftragten und dem Unternehmen helfen, die sich aus der DSGVO ergebenden Verpflichtungen zu erfüllen, und sicherstellen, dass alle Verarbeitungsaktivitäten personenbezogener Daten auf legale und transparente Weise durchgeführt werden und für die betroffenen Personen verständlich sind.

Verarbeitungsaktivität:

Nr:

1) Allgemeines

1.1 Verarbeitungsaktivitäten

Welche Verarbeitungsaktivität/en (Aktivität/en) werden bewertet?

Auf der Verallia Mitarbeiterplattform werden allgemeine Informationen zum Unternehmen allen Mitarbeiterinnen und Mitarbeitern der Verallia Deutschland AG zur Verfügung gestellt.

1.2 Beschreibung

Bitte beschreiben Sie die durchgeführte Tätigkeit

Zum Beispiel:

- Was machen Sie und warum?

Unternehmensinformationen werden auf der Verallia Mitarbeiterplattform veröffentlicht und allen Mitarbeitern der Verallia Deutschland AG zur Verfügung gestellt.

- Welcher ist der Kontext / Hintergrund?

Besserer Informationsaustausch besonders mit Mitarbeiterinnen und Mitarbeitern ohne Verallia-Mailadresse.

- Wer ist der zuständige Verantwortliche?

Elisa Sauter und Cornelia Banzhaf

- Wie üben Sie Ihre Tätigkeit aus?

Unternehmenskommunikation und Nachhaltigkeit

- Welche Ressourcen werden verwendet?

Pimcore (Content Management System) und Evalanche (Datenverwaltungssystem)

1.3 Zweck(e) der Verarbeitung / Verarbeitungskategorien

Was ist der Zweck / Verwendungszweck der Verarbeitung?

Informationen werden mit allen Mitarbeiterinnen und Mitarbeitern geteilt. Insbesondere auch eine bessere Erreichbarkeit der Werke und damit der Mitarbeiter ohne Verallia-Mailadresse.

1.4 Verantwortlicher für das Projekt

Wer ist der zuständige Verantwortliche für das Projekt im Unternehmen?

Bitte geben Sie den Namen, die Kontaktdaten, die Abteilung und die Betriebseinheit der zuständigen Person an.

Cornelia Banzhaf

PR Manager

+49 7564 18 255

Cornelia.banzhaf@verallia.com

Elisa Sauter

Specialist Communication & CSR

+49 7564 18 260

Elisa.sauter@verallia.com

1.5 Auftragsverarbeiter

Ist Verallia in diesem Prozess als Auftragsverarbeiter tätig?

Auftragsverarbeiter - eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Ja Nein ✖

1.6 Vertrag / Dienstleistungsvertrag

Besteht ein Dienstleistungsvertrag zwischen den am Prozess beteiligten Parteien bzw. Unternehmen?

Wir beabsichtigen zu überprüfen, ob dieser Dienstleistungsvertrag in schriftlicher Form vorliegt.

Ja ✖ Nein

Bitte begründen Sie Ihre Antwort:

1.7 Unterauftragsvereinbarung

Besteht eine Unterauftragsvereinbarung zwischen den am Prozess beteiligten Parteien bzw. Unternehmen?

Art. 28 der DSGVO sieht vor, dass die Datenverarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments erfolgt bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Ja Nein Trifft nicht zu ✖

Bitte begründen Sie Ihre Antwort:

1.8 Vertragliche Regelungen / Bestimmungen – Art.º 28.º

Bitte geben Sie an, welche der folgenden Optionen in der Unterauftragsvereinbarung vorgesehen sind (Punkt 1.7):

Vertragsbestandteile Allgemein:

1. Schriftlicher Vertrag:
2. Gegenstand und Dauer des Auftrags:
3. Art und Zweck der Verarbeitung/ Datenverarbeitung:
4. Art der personenbezogenen Daten:
5. Kategorien betroffener Personen:
6. Technische und organisatorische Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO:
7. Rechte des Verantwortlichen (Kontrollen):
8. Dokumentierte Weisung/ Weisungsbefugnisse des Verantwortlichen im Hinblick auf die Verarbeitung personenbezogener Daten:

Pflichten des Auftragsverarbeiters

1. Möglichkeit weitere Auftragsverarbeiter in Anspruch zu nehmen (Berechtigung von Unterauftragsverhältnissen):
2. Informationspflicht über Änderungen von Sub-Unternehmen:
3. Mitteilungen über Datenschutzvertöße:
4. Verschwiegenheitsverpflichtung der Mitarbeiter:
5. Auskunftserteilung zum Zweck des Nachweises der Einhaltung von Verpflichtungen:
6. Rückgabe bzw. Löschung der Daten nach Beendigung des bestehenden Vertragsverhältnisses:

1.9 Betroffene Personen und personenbezogene Daten

Welche personenbezogenen Daten sind betroffen?

Bitte geben Sie die Gruppen der betroffenen Personen an, deren personenbezogenen Daten Sie verarbeiten, und wählen Sie für jede Gruppe die Kategorien der behandelten Daten und verarbeitete Datenelemente aus.

1.10 Öffentlich zugängliche Daten

Sind die in diesem Projekt behandelten personenbezogenen Daten öffentlich zugänglich?

HINWEIS: Wenn personenbezogenen Daten bereits erfasst wurden, waren sie zum Zeitpunkt der Erfassung der Öffentlichkeit zugänglich?

Ja Nein ✖ Ich bin mir nicht sicher

Bitte begründen Sie Ihre Antwort:

1.11 Vorherige Datenschutzfolgenabschätzung

Würden Sie die Art, den Umfang, die Umstände und die Zwecke dieser Verarbeitung als ähnlich betrachten, als eine andere Verarbeitung, für die bereits eine DSFA durchgeführt wurde?

Ja Nein Ich bin mir nicht sicher ✖

Bitte begründen Sie Ihre Antwort:

1.12 Rechtsgrundlage

Welche der folgenden Optionen ermöglicht es Ihnen Daten für diese Datenverarbeitung zu verwenden?

Sie können zusätzliche Informationen bereitstellen / hinzufügen.

Wenn Sie sich bei der Beantwortung dieser Frage nicht sicher sein sollten, wählen Sie bitte "Ich bin (mir) nicht sicher" und geben Sie alle Informationen an, die Sie für relevant halten.

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten gegeben;

✖ Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich;

- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

- Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

- Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt;

- Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen;

- Ich bin (mir) nicht sicher

1.13 Berechtigte Interessen – Logik

Haben Sie als Rechtsgrundlage für die Verarbeitung in Frage 1.12 „Wahrung der berechtigten Interessen" gewählt?

Ja ✖ Nein

1.14 Berechtigte Interessen

Wenn Sie bei der Antwort auf Frage 1.13 "Ja" gewählt haben, geben Sie bitte an, welche berechtigte Interessen vorliegen.

Sie können zusätzliche Informationen bereitstellen, die Sie für relevant halten.

Wenn Sie sich bei der Beantwortung dieser Frage nicht sicher sein sollten, wählen Sie bitte "Ich bin (mir) nicht sicher" und geben Sie alle Informationen an, die Sie für relevant halten.

- Direktmarketingzwecke;

- Vorbeugung von Betrug;

- Übermittlung von Beschäftigtendaten innerhalb des Konzerns bzw. Unternehmensgruppe für interne Verwaltungszwecke;

- Gewährleistung der Netz- und Informationssicherheit;

- Unautorisierten Zugang zu elektronischen Kommunikationsnetzen verhindern/unterbinden;

- Schädigungen von Computer- und elektronischen Kommunikationssystemen abwehren;

- Hinweis auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit an eine zuständige Behörde;

- Verarbeitung / Abwicklung von Zahlungen oder Abonnements, um finanzielle Verpflichtungen oder Verträge zu erfüllen;

- Ich bin mir nicht sicher;

- Andere;

✖ Trifft nicht zu.

Bitte begründen Sie Ihre Antwort:

1.15 Analyse der berechtigten Interessen

Bitte erläutern Sie, warum die berechtigten Interessen nicht gegen grundlegende Interessen oder Rechte und Freiheiten der betroffenen Personen verstoßen.

Bitte berücksichtigen Sie die angemessenen Erwartungen der betroffenen Personen hinsichtlich der Verwendung ihrer personenbezogenen Daten. Anders formuliert: war den betroffenen Personen bekannt, zum Zeitpunkt und im Kontext der Erhebung personenbezogener Daten, dass eine Datenerfassung zu diesem Zweck erfolgen könnte?

- Ich bin mir nicht sicher
- Bitte begründen Sie Ihre Antwort:

1.16 Bewertung und Evaluierung

Umfasst die Datenverarbeitung Kriterien für die Bewertung und Evaluierung?

Beispielsweise:

- ein Finanzinstitut, das seine Kunden gegen eine Kreditreferenzdatenbank oder gegen eine Datenbank zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung oder Betrug prüft;

- uma empresa de biotecnologia que oferece testes genéticos diretamente aos consumidores de modo a analisar e predizer os riscos de doença/saúde; ou

- Ein Biotechnologieunternehmen, das ihre Gentests den Verbrauchern direkt anbietet, um mögliche Krankheits- und Gesundheitsrisiken zu analysieren bzw. vorherzusagen; oder

- Ein Unternehmen, das anhand der Nutzung seiner Website Verhaltens- oder Marketingprofile seiner Websitebesucher erstellt.

Ja Nein ✖ Ich bin mir nicht sicher

Bitte begründen Sie Ihre Antwort unten:

1.17 Automatisierte Entscheidungsfindung

Umfasst die Datenverarbeitung die Anwendung von automatisierten Entscheidungsprozesse?

Beispielsweise:

- wenn eine betroffene Person einen Online-Kreditantrag beantragt und die Website eine sofortige automatisierte Entscheidung auf der Grundlage von Algorithmen und einer Bonitätsprüfung liefert;

- wenn das Gehalt eines Arbeitnehmers automatisch - basierend auf einer automatisierten Verarbeitung seiner Produktivität angepasst wird; oder

- Eine Verarbeitung, die zum Ausschluss oder zur Diskriminierung betroffenen Personen führen kann.

HINWEIS: Dies schließt keine Verarbeitung ein, die keine oder nur geringe Auswirkungen auf die betroffenen Personen hat.

Ja Nein ✖ Ich bin mir nicht sicher

Bitte begründen Sie Ihre Antwort unten:

1.18 Automatisierte Entscheidungsfindung – Grundlage

Welche der folgenden Optionen erlaubt es Ihnen Daten für eine automatisierte Entscheidungsfindung (oder Profilbildung) zu verwenden?

- Für die Erfüllung eines Vertrages mit der betroffenen Person erforderlich;

- Ist von der EU oder einem Gesetz eines Mitgliedstaats zugelassen;

- Beruht auf der ausdrücklichen Zustimmung der betroffenen Person;

- Ich bin mir nicht sicher

Bitte begründen Sie Ihre Antwort unten:

1.19 Regelmäßige und systematische Überwachung

Umfasst die Aktivität die regelmäßige und systematische Überwachung eines öffentlich zugänglichen Bereichs?

Eine "systematische Überwachung" bedeutet Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel hat;

Ein "öffentlich zugänglicher Bereich" ist ein Ort, der allen Mitgliedern der Öffentlichkeit zugänglich ist.

Zum Beispiel, Videoüberwachungsanlagen i.e. Überwachungskameras an/in

- einem Platz;

- einem Einkaufszentrum;

- einer Straße oder

- in einer öffentlichen Bibliothek

Ja Nein ✖ Ich bin mir nicht sicher

Bitte begründen Sie Ihre Antwort unten:

1.20 Vertrauliche Daten

Umfasst die Aktivität die Verarbeitung der unten aufgeführten sensiblen/ vertraulichen Daten?

Wenn die Verarbeitung keine der folgenden Optionen umfasst, wählen Sie "nicht zutreffend."

- Daten, die die rassische oder ethnische Herkunft offenbaren;
- Daten, die die politische Meinungen offenbaren;
- Daten, die religiöse oder philosophische Überzeugungen offenbaren;
- Daten, die eine Gewerkschaftszugehörigkeit belegen/offenbaren
- Genetische Daten;
- Biometrische Daten;
- Gesundheitsdaten;
- Daten betreffend sexuelles Verhalten;
- Daten über die sexuelle Orientierung oder Geschlechtsidentität;
- Daten über strafrechtliche Verurteilungen oder Straftaten;
- Elektronische Kommunikationsdaten;
- Standortdaten;
- Finanzdaten;

☒ nicht zutreffend.

1.21 Umfangreiche Verarbeitung

Liegt eine umfangreiche Datenverarbeitung vor?

Die folgenden Punkte müssen berücksichtigt werden, damit geklärt werden kann, ob eine umfangreiche Verarbeitung vorliegt oder nicht:

- Die Zahl der betroffenen Personen – entweder als spezifische Zahl oder als Anteil an der maßgeblichen Bevölkerung;

- Das Datenvolumen und/oder die Bandbreite der verarbeiteten Datenelemente;

- Die Dauer oder Permanenz der Datenverarbeitungstätigkeit;

- Die geografische Ausdehnung der Verarbeitungstätigkeit;

Beispiele für eine umfangreiche Verarbeitung stellen dar:

- die Verarbeitung von Patientendaten im gewöhnlichen Geschäftsbetrieb eines Krankenhauses;

- die Verarbeitung von Reisedaten natürlicher Personen, die das öffentliche Verkehrssystem einer Stadt nutzen (z. B. Überwachung über Fahrkarten);

- die Verarbeitung von Geolokalisierungsdaten von Kunden einer internationalen Fast-food-Kette in Echtzeit zu statistischen Zwecken durch einen auf Tätigkeiten dieser Art spezialisierten Auftragsverarbeiter; oder

- die Verarbeitung personenbezogener Daten durch eine Suchmaschine zu Zwecken der verhaltensbasierten Werbung;

Keine umfangreiche Verarbeitung stellen die folgenden Beispiele dar:

- die Verarbeitung von Patientendaten durch einen einzelnen Arzt;

- die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten durch einen einzelnen Rechtsanwalt.

Ja Nein ✖ Ich bin mir nicht sicher

1.22 Abgleichen oder Zusammenführen von Datensätzen

Beabsichtigt die zu analysierende Aktivität, Datensätze abzugleichen oder zu kombinieren?

Zum Beispiel:

- eine Universität, die akademische Studentenakten mit sportlichen Studentenakten kombiniert;

- eine Versicherungsgesellschaft, die Krankenakten und Kundenauftragsdaten kombiniert;

- Behörden, die Gesichtserkennungsdaten mit der Analyse von Fingerabdrücken abgleichen und kombinieren; oder

- die Erfassung von Daten aus öffentlichen sozialen Netzwerken, um Profile zu erstellen.

Ja Nein ✖ Ich bin mir nicht sicher

1.23 Daten schutzbedürftiger betroffener Personen

Werden Daten schutzbedürftiger betroffener Personen verarbeitet?

In "Andere" können Sie jeden Fall einbeziehen, in dem ein Ungleichgewicht / ein unausgewogenes Machtverhältnis in der Beziehung zwischen dem Individuum und der Unternehmen besteht.

Sie können zusätzliche Informationen bereitstellen, die Sie für relevant halten.

Wenn Sie sich bei der Beantwortung dieser Frage nicht sicher sind, wählen Sie bitte "Ich bin mir nicht sicher" und fügen Sie alle relevanten Informationen in das Feld „Notizen" unten ein.

- Arbeitnehmer, Kinder oder andere Personen mit besonderem Schutzbedarf (psychisch Kranke);

- Asylbewerber;

- Senioren, Nutzern von Gesundheitsdienstleistungen.

Ich bin mir nicht sicher Trifft nicht zu ✖ Andere:

Notizen:

1.24 Neue Technologien

Beinhaltet der Verarbeitungsvorgang eine innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen? Wenn ja, welche?

Zum Beispiel:

- Kombination aus Fingerabdruck- und Gesichtserkennung zum Zweck einer verbesserten Zugangskontrolle; oder

- bestimmte „Internet der Dinge"– Anwendungen, z. B. miteinander verbundene (oder "intelligente") Geräte, Privathaushalte oder Städte.

Ja Nein ✖ Ich bin mir nicht sicher

1.25 Hinderung der Ausübung der Rechte der betroffenen Personen

Kann die Datenverarbeitung die betroffenen Personen (potentiell) an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern?

Hierzu gehören:

- Die Verarbeitung der Daten erfolgt in einem öffentlichen Bereich, wo Personen nicht umhin können (Einschränkung ihrer Rechte); oder

- Verarbeitung, die darauf zielt, den Zugang betroffener Personen zu einem Dienst oder zum Abschluss eines Vertrags zu erlauben, ändern oder verweigern.

Zum Beispiel:

- Durchsuchen von Bonitätsdatenbanken zum Zweck der Entscheidung, ob ein Kredit vergeben wird. OU Eine Bank, die ihre Kunden gegen eine Kreditreferenzdatenbank prüft, um über Kreditvergaben zu entscheiden.

Ja Nein ✖ Ich bin mir nicht sicher

1.26 Bewertung der Notwendigkeit

Wie notwendig ist diese Aktivität / Verarbeitungsvorgang in Bezug auf ihren Zweck?

- Kritisch
- Sehr hoch

✖ Hoch

- Mittel
- Gering
- Sehr gering
- Unnötig
- Ich bin mir nicht sicher

- Trifft nicht zu

Kann der Zweck durch andere Mittel erreicht werden, die weniger in die Privatsphäre eingreifen?

Ja Nein ✖

1.27 Vorteile – Details

Was sind die Vorteile dieser Aktivität / dieses Verarbeitungsvorgangs?

✖ Zugang zu Ressourcen;

✖ Kommunikation;

- Bequemlichkeit – Annehmlichkeit;
- Kostensenkung;
- Kundenzufriedenheit;
- Bildung;
- Effizienz;
- Energieeinsparung;
- Unterhaltung;
- Umwelt;
- Finanzielles Wachstum;
- Betrugsvorbeugung;
- Gesundheit und Wohlbefinden;

✖ Informationssicherheit;

- Innovation;
- Kenntnis - Wissen;
- Persönliche Entwicklung;
- Physische Sicherheit;
- Produktivität;

✖ Weiterbildung;

- Öffentliches Wohlergehen/ Gemeinwohl;
- Sicherheit;
- Wissenschaftliche Forschung;
- Diebstahlprävention / Verhinderung von Diebstahl

Ich bin mir nicht sicher Trifft nicht zu Andere:

1.28 Vorteile – Unternehmen

Wer profitiert von dieser Aktivität / von diesem Verarbeitungsvorgang?

✖ Die Organisation / Firma selbst;

✖ Betroffene Personen;

- Gesellschaft.

Ich bin mir nicht sicher Trifft nicht zu Andere

1.29 Schäden – Details

Kann die Aktivität oder ein möglicher Verstoß gegen personenbezogene Daten den betroffenen Personen einen der folgenden Schäden zufügen?

- Diskriminierung;

✖ Identitätsdiebstahl;

- Betrug;

- Finanzieller Schaden;

- Reputationsschaden;

- Verschwiegenheitsverletzung - Verlust der Vertraulichkeit;

- Nicht autorisierte Rückführung der Pseudonymisierung;

- Erhebliche soziale oder wirtschaftliche Nachteile;

- Entzug individueller Rechte und Freiheiten;

- Hinderung der Kontrolle über eigene Daten;

- Es ist unwahrscheinlich, dass durch die Aktivität Schäden entstehen;

- Ich bin mir nicht sicher.

Trifft nicht zu Andere:

1.30 Schäden - Ursachen

Was sind die möglichen Ursachen für diese Schäden?

✖ Datenschutzverletzung;

- Übeltäter;

- Kriminelle Aktivität;

- Mangelhafte Überwachung / mangelhaftes Monitoring;

- Unangemessene Richtlinien / Verfahren;

- Ungeschützte Speicherung / Lagerung;

- Unzureichende Rechenschaftspflicht / Verantwortung;

- Mangel an umfassender Erfahrung;

- Unzureichende Tests;

- Unzureichende Ausbildung;

- Störung oder Ausfall der Geräte;

- Ich bin mir nicht sicher.

Trifft nicht zu Andere:

1.31 Schäden - Besonderheiten

Welche besondere Kategorien betroffener Personen sind von diesen Schäden betroffen?

- Kunden/ Benutzer,

-Lieferanten,

✖Mitarbeiter;

- Potenzielle Mitarbeiter;

- Nutzern von Gesundheitsdienstleistungen;

- Studenten.

Ich bin mir nicht sicher Trifft nicht zu Andere

1.32 Schadenswahrnehmung

Wie können diese potenziellen Schäden aus Sicht der betroffenen Personen betrachtet werden?

Ich weiß es nicht Ich bin mir nicht sicher ✖

1.33 Meinungen der betroffenen Personen

Hatten die an der Verarbeitung beteiligten betroffenen Personen die Möglichkeit, ihre Meinung zu der Aktivität / zum Verarbeitungsvorgang zu äußern?

Dies kann auch einen Vertreter der betroffenen Person sein.

Ja Nein ✖ Ich bin mir nicht sicher Trifft nicht zu

1.34 Kategorien von Empfängern

Wer (Behörden, Unternehmen) kann auf die Daten zugreifen?

Die Kenntnis darüber, welche Parteien/ Unternehmen Zugang zu personenbezogenen Daten haben, ist ein entscheidender Faktor für die Aufbewahrung, Verarbeitung und Begrenzung personenbezogener Daten.

Ich bin mir nicht sicher Trifft nicht zu ✖

1.35 Standort der Empfänger

Wo befindet sich der Standort des Empfängers und aller beteiligten Parteien geografisch?

✖ Innerhalb der EU (bitte geben Sie das Land an)

Außerhalb der EU (bitte geben Sie das Land an)

Ich bin mir nicht sicher Trifft nicht zu

1.36 Grenzüberschreitende Übermittlung

Werden Daten außerhalb der Europäischen Union / des Europäischen Wirtschaftsraums übertragen / übermittelt?

Europäische Union (EU)

Europäischer Wirtschaftsraum (EWR)

Ja Nein Ich bin mir nicht sicher Trifft nicht zu

1.37 Mechanismen für grenzüberschreitende Übermittlungen

Welche Mechanismen gibt es, um personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums (EWR) an ein Drittland zu übertragen (falls zutreffend)?

Die Übermittlung personenbezogener Daten außerhalb des Europäischen Wirtschaftsraums an Drittländer unterliegt Kapitel V. der DSGVO, das andere anwendbare Datenübertragungsmechanismen fordert.

- Angemessenheitsentscheidung;

- Ein rechtsverbindliches und durchsetzbares Instrument zwischen Behörden oder Stellen selbst;

- Verbindliche Unternehmensregeln;

- Angenommene Standarddatenschutzklauseln (Standarddatenschutzklauseln, die von einer Aufsichtsbehörde angenommen und von der Kommission genehmigt wurden);

- Einen genehmigten Verhaltenskodex;

- Ein zugelassener Zertifizierungsmechanismus;

- Genehmigung durch die zuständige Aufsichtsbehörde;

- Ausdrückliche Einwilligung der betroffenen Person;

- Die Übertragung ist zur Erfüllung eines Vertrages mit der betroffenen Person erforderlich;

- Die Übertragung ist aus Gründen des öffentlichen Interesses erforderlich;

- Die Übertragung wird zur Ausübung oder Verteidigung von Rechtsansprüchen benötigt;

ist für die Ausübung oder Verteidigung eines Rechts in einem Gerichtsverfahren erforderlich;

- Die Übertragung ist erforderlich, um die vitalen Interessen der betroffenen Person oder einer anderen natürlichen Person zu verteidigen.

- Angemessene Schutzmaßnahmen nach Artikel 49 Absatz 1 der DSGVO;

Ich bin mir nicht sicher Trifft nicht zu ✖

2) Verarbeitung (personenbezogenen Daten)

2.1 Fairness und Gerechtigkeit

Welche Schritte haben Sie unternommen, um sicherzustellen, dass die personenbezogenen Daten fair und gerecht verarbeitet wurden?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

✖ Standardmäßig sind die Datenschutzeinstellungen der Benutzer für diese am günstigsten;

- Benutzer werden über vordefinierte Datenschutzeinstellungen - und wie Sie diese ändern können – informiert;

- Datenschutztools, Datenschutz-Einstellungen und -Funktionen sind verständlich, klar erkennbar, leicht zugänglich und intuitiv zu bedienen.

Ich bin mir nicht sicher Trifft nicht zu Andere:

2.2 Grundsatz der Transparenz

Welche Maßnahmen wurden ergriffen, um sicherzustellen, dass personenbezogene Daten transparent erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

✖ Benutzer werden darüber informiert, wer ihre Daten sammelt / verwendet;

- Benutzer haben die Möglichkeit, Probleme, Bedenken/Zweifel zu melden;

- Benutzer erhalten ein Datenschutz-Dashboard;

- Den Benutzern werden Ergänzungen für den Webbrowser zur Verfügung gestellt, die bei Datenschutzfragen behilflich sind; Benutzer erhalten Ergänzungen für den Webbrowser, die bei Datenschutzfragen behilflich sind;

- Benutzer können Informationen zum Datenschutz, zu datenschutzspezifische Zertifizierungen und Datenschutzsiegel sowie Datenschutzprüfzeichen einsehen.

Ich bin mir nicht sicher Trifft nicht zu Andere:

2.3 Grundprinzip der Zweckbindung

Welche Schritte/Maßnahmen haben Sie unternommen, um sicherzustellen, dass Daten nur für bestimmte, ausdrückliche und legitime Zwecke erhoben und verwendet werden?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

✖ Der Zweck jeder Datenverarbeitung wird vor der Erfassung festgelegt.

- Für jede Verarbeitung personenbezogener Daten ist ein eindeutiger Verwendungszweck angegeben/aufgeführt.

- Personenbezogene Daten werden niemals "nur für den Fall" gesammelt.

Ich bin mir nicht sicher Trifft nicht zu Andere

2.4 Einschränkung der Nutzung

Welche Schritte/Maßnahmen haben Sie unternommen bzw. veranlasst, um sicherzustellen, dass personenbezogene Daten nicht auf eine Weise verarbeitet werden, die mit diesen Zwecken nicht vereinbar sind?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

✖ Die Verarbeitungs-, Nutzungs -und Übermittlungsrechten sind eingeschränkt;

✖ Die bestehenden Unternehmensrichtlinien minimieren das Risiko vor Hacker-Angriffen;

- Qualitätssichernde Revisionen gewährleisten Compliance bei der Softwareentwicklung;

- Es besteht eine Trennung nach Organisations-/Abteilungsgrenzen;

- Es besteht eine Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens;

- Es werden zweckspezifische Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten verwendet/eingesetzt;

- Es werden geregelte Zweckänderungsverfahren angewendet / Es gibt geregelte Zweckänderungsverfahren

Ich bin mir nicht sicher Trifft nicht zu Andere:

2.5 Zusätzliche Zwecke

Zu welchen zusätzlichen Zwecken werden personenbezogenen Daten verarbeitet?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

Wenn die Daten nicht für zusätzliche Zwecke verarbeitet werden, wählen Sie „Nicht zutreffend."

- Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken;

- Verarbeitung zu wissenschaftlichen Forschungszwecken;

- Verarbeitung zu historischen Forschungszwecken;

- Verarbeitung zu statistischen Zwecken.

Ich bin mir nicht sicher Trifft nicht zu ✖ Andere:

2.6 Datenminimierung

Welche Schritte haben Sie unternommen, um sicherzustellen, dass die gesammelten Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

- Die Daten werden gemäß eines festgelegten/verfolgten Zweckes gesammelt;

✖ Es werden nicht mehr Daten gesammelt, als zur Erreichung eines festgelegten Zwecks erforderlich ist;

- Die Verarbeitung von Daten ist auf das zur Erreichung des Verarbeitungszwecks erforderliche Minimum zu beschränken.

- Automatische Sperr- und Löschmechanismen wurden implementiert;

- Die Benutzeroberfläche unterscheidet zwischen optionalen und erforderlichen Feldern;

- Die Verwendung von Freiform-Textfeldern wird vermieden;

- Definierte Felder (z. B. Dropdown- / vorab ausgefüllte Listen usw.) werden gegenüber Freiformfeldern bevorzugt.

Ich bin mir nicht sicher Trifft nicht zu Andere:

2.7 Datenqualität – Genauigkeit

Welche Schritte haben Sie unternommen, um sicherzustellen, dass die Daten korrekt sind?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

✖ Es sind Kontrollmöglichkeiten vorhanden, um die Richtigkeit und Qualität der Daten regelmäßig zu überprüfen;

✖ Es gibt Validierungskontrollen, um inkonsistente, unvollständige und ungenaue Daten herauszufiltern.

Ich bin mir nicht sicher Trifft nicht zu Andere:

2.8 Datenqualität –Aktualisierung

Welche Schritte haben Sie unternommen, um sicherzustellen, dass die Daten auf dem neuesten Stand sind?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

✖ Es gibt Kontrollmöglichkeiten, um die Aktualisierung und Qualität der Daten regelmäßig zu überprüfen;

✖ Es gibt Validierungskontrollen, um alte Daten herauszufiltern;

✖ Alte Daten werden gelöscht oder aktualisiert.

Ich bin mir nicht sicher Trifft nicht zu Andere:

2.9 Einschränkung der Datenspeicherung

Welche Schritte haben Sie unternommen, um sicherzustellen, dass die Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist?

Bitte wählen Sie eine der folgenden Optionen und / oder fügen Sie Ihre eigenen hinzu:

ANMERKUNG: In einigen Fällen können Daten länger aufbewahrt werden, wenn ihre Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen und historischen Forschungszwecken oder zu statistischen Zwecken unterliegt. Es muss jedoch immer sichergestellt werden, dass geeignete technische und organisatorische Maßnahmen bestehen, die die Rechte und Freiheiten der betroffenen Person gewährleisten.

✖ Es bestehen Verfahren zur regelmäßigen Überprüfung der Bestandsaufnahme der verfügbaren Daten (Überprüfen des Dateninventars) und zum Eliminieren der Prozesse.

- Es besteht eine zeitliche Begrenzung für die Speicherung von Daten und Tools zur Löschung von personenbezogenen Daten;

✖ Alle persönlichen Daten werden gelöscht, wenn das Konto eines Benutzers deaktiviert / gelöscht wird.

Ich bin mir nicht sicher Trifft nicht zu Andere:

2.10 Aufbewahrungsfristen

Beschreiben Sie die Dauer der Aufbewahrungsfristen personenbezogenen Daten.

Wie lange werden Sie die für den im Projekt verfolgten Zweck gesammelte Daten speichern und aufbewahren?

Ich bin mir nicht sicher Trifft nicht zu Andere ✖

Mit Austritt aus dem Unternehmen bzw. Ende der Betriebszugehörigkeit werden die Daten gelöscht.

2.11 Benachrichtigung der betroffenen Personen

Wird die betroffene Person über die durchgeführte Datenverarbeitung benachrichtigt?

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

2.12 Benachrichtigung der betroffenen Personen - Inhalt

Entspricht die Benachrichtigung / Information an die betroffene Person allen unten genannten Anforderungen?

- Ist sie präzise und transparent;
- Ist sie verständlich;
- Ist sie leicht zugänglich;
- Ist sie deutlich und unmissverständlich;
- Wird diese schriftlich oder auf andere Weise vorgelegt;
- Ist sie kostenlos.

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

2.13 Benachrichtigung – juristische/rechtliche Überprüfung

Wurde die Benachrichtigung/Mitteilung vom Datenschutzteam - Rechtsteam überprüft, um die Einhaltung aller geltenden Gesetze sicherzustellen?

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

2.14 Zustimmung/Einwilligung

Haben Sie "Einwilligung/Zustimmung" als Rechtsgrundlage für die Verarbeitung gewählt?

Ja ✖ Nein

2.15 Einwilligungserklärung / Einverständniserklärung

Entspricht die Einverständniserklärung ALLEN unten aufgeführten Anforderungen?

- Diese unterscheidet sich deutlich von anderen Sachverhalten;
- Ist verständlich dargestellt und leicht zugänglich;
- Sprache ist präzise, unmissverständlich und deutlich.

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

2.16 Einwilligung des Betroffenen – Beifügungen

Die Einwilligungserklärung umfasst / beinhaltet ALLE der folgenden Anforderungen?

- Diese wurde frei geäußert;
- Es handelt sich um eine spezifische und informierte Zustimmung;
- Diese ist eindeutig und unmissverständlich.

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

2.17 Zustimmung/Einwilligung - Nachweis

Ist es möglich nachzuweisen, dass die Einwilligung ordnungsgemäß eingeholt wurde und alle in den vorstehenden Fragen genannten Anforderungen erfüllt?

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

2.18 Widerruf der Einwilligung

Ist der Widerruf der Einwilligung seitens der betroffenen Person so einfach wie die Erteilung der Einwilligung?

Wenn die Einwilligung beispielsweise elektronisch durch ein Mouse-Klick bzw. durch das Drücken einer Taste eingeholt wurde, muss es genauso einfach sein, die Einwilligung zu widerrufen.

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

2.19 Einwilligung - Kinder

Wird die Zustimmung der Eltern oder der Erziehungsberechtigten eingeholt, bevor Daten von einem Kind unter 16 Jahren erhoben/verarbeitet werden?

HINWEIS: Dies gilt nur, wenn die Verarbeitung mit der Bereitstellung von Informationen zusammenhängt, die die Gesellschaft einem Kind direkt zuweist (z. B. E-Commerce, ISPs, Suchmaschinen, soziale Netzwerke usw.).

Ja Nein Ich bin mir nicht sicher Trifft nicht zu ✖

3) Rechte der betroffenen Person

3.1 Informationspflicht - Recht auf Auskunft zu personenbezogenen Daten

Kann eine Mitteilung oder Benachrichtigung, die einer Datenschutzprüfung i.e. einer rechtlichen Überprüfung unterzogen wird, vorgelegt verwendet werden, um die betroffenen Personen zu informieren, wie ihre Daten behandelt werden?

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

3.2 Recht auf Auskunftserteilung

Gibt es Mechanismen, mit denen betroffene Personen den Zugriff auf die über sie verarbeiteten personenbezogenen Daten anfordern können?

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

3.3 Recht auf Berichtigung

Besteht die Möglichkeit für betroffene Personen, die Korrektur unrichtiger Daten als auch die Vervollständigung oder Ergänzung unvollständiger Daten anzufordern?

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

3.4 Recht auf Datenlöschung ("Recht auf Vergessenwerden")

Gibt es Mechanismen, um personenbezogene Daten auf Anfrage der betroffenen Personen zu löschen?

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

3.5 Recht auf Einschränkung der Verarbeitung

Besteht die Möglichkeit, die Verarbeitung der Daten auf Anfrage der betroffenen Person einzuschränken?

Ja ✖ Nein Ich bin mir nicht sicher Trifft nicht zu

3.6 Recht auf Datenübertragbarkeit

Gibt es eine Möglichkeit, personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format an die betroffene Person oder einer anderen Partei zu übertragen?

„Maschinenlesbares Format" bedeutet:

„Daten in einem Format, das von einem Computer / Computerprogramm automatisch gelesen und verarbeitet werden kann, z. B. CSV, JSON, XML usw. Maschinenlesbare Daten müssen strukturierte Daten sein." (EU-Glossar)

„Vom Menschen lesbare Daten" bedeutet:

"Daten in einem Format, das von Menschen bequem gelesen werden kann. Einige davon, wie z. B. PDF, werden nicht automatisch gelesen, da es sich nicht um strukturierte Daten handelt, dh. die Darstellung der Daten auf der Festplatte stellt nicht die aktuellen Beziehungen dar, die in den Daten vorhanden sind." (EU-Glossar)

Ja Nein ✖ Ich bin mir nicht sicher Trifft nicht zu

3.7 Widerspruchsrecht

Gibt es Mechanismen, die es betroffenen Personen ermöglicht, sich gegen die Verarbeitung sie betreffender personenbezogener Daten zu widersetzen i.e. Widerspruch einzulegen?

Ja Nein ✖ Ich bin mir nicht sicher Trifft nicht zu

3.8 Recht, sich keiner automatisierten Entscheidung zu unterwerfen

Besteht für die betroffenen Personen die Möglichkeit eine ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung anzufechten?

Zum Beispiel:

- eine automatisierte Entscheidung über einen Online-Kreditantrag abzulehnen, die ausschließlich auf Algorithmen und Kreditrecherchen basiert;

- ein Arbeitnehmer lehnt eine automatisierte Entscheidung ab, die sein Gehalt entsprechend einer automatisierten Überwachung seiner Produktivität automatisch anpasst.

Dies schließt / umfasst keine Verarbeitung ein, die keine oder nur geringe Auswirkungen auf die betroffenen Personen hat.

Ja Nein ✖ Ich bin mir nicht sicher Trifft nicht zu

4) Technische und organisatorische Maßnahmen

4.1 Ressourcen/Quellen

Aus welchen Bestände/ Datenbestände (Ressourcen/Quellen) stammen die personenbezogenen Daten?

Mit anderen Worten, was verwenden Sie, um die Daten zu erhalten/erheben?

Eine Ressource unterstützt informationsbezogene Aktivitäten.

Ressourcen/Quellen können Softwaresysteme, Anwendungen, Datenbanken oder sogar Dateien umfassen.

Ich bin mir nicht sicher Trifft nicht zu Andere: ✖ (siehe Excel-Liste)

4.2 Technische und organisatorische Maßnahmen – Ressourcen

Welche technische und organisatorische Maßnahmen wurden zum Schutz der personenbezogenen Daten in Bezug auf diese Ressource/Quelle getroffen?

ICRF Kontrolle

Ich bin mir nicht sicher Trifft nicht zu

4.3 Ressourcen zur Aufbewahrung

Welche Ressourcen werden für die Datenverarbeitung bei dieser Aktivität gebraucht?

Mit anderen Worten, wo werden die Daten nach der Erfassung gesammelt? Evalanche

Bleiben die Daten beweglich oder werden sie bewegt? Nein

Eine Ressource unterstützt informationsbezogene Aktivitäten.

Ressourcen können Softwaresysteme, Anwendungen, Datenbanken oder sogar Dateien umfassen.

Ich bin mir nicht sicher Trifft nicht zu Andere:

4.4 Zielressourcen

Welche technische und organisatorische Maßnahmen schützen die Daten in Bezug auf diese Ressource?

ICRF Handbuch

Ich bin mir nicht sicher Trifft nicht zu

4.5 Sicherheitserwägungen

Haben Sie bei der Auswahl Ihrer Sicherheitsmaßnahmen Folgendes berücksichtigt?

☒ Aktueller Stand der Technik;

☒ Kosten der Implementierung;

- Art der Verarbeitung;

- Umfang der Verarbeitung;

- Kontext der Verarbeitung;

☒ Zwecke der Verarbeitung;

- Risiko der variierenden Wahrscheinlichkeit und Schwere der Verletzung der Rechte und Freiheiten natürlicher Personen.

Ich bin mir nicht sicher Andere

4.6 Verhaltensregeln

Kennen Sie die genehmigten Verhaltenskodizes, mit denen sich ihr Unternehmen verpflichtet hat?

Hierzu gehören:

Verhaltenskodizes, die von Verbänden oder Vertretungsorganen erstellt und von einer EU-Aufsichtsbehörde, dem Europäischen Datenschutzausschuss (EDSA) oder der Europäischen Kommission zum Zwecke der Einhaltung der DSGVO genehmigt wurden.

Ja ☒ Nein Ich bin mir nicht sicher Trifft nicht zu

5) Zusätzliche Information

Bitte fügen Sie weitere Informationen zu, die Sie für relevant halten:

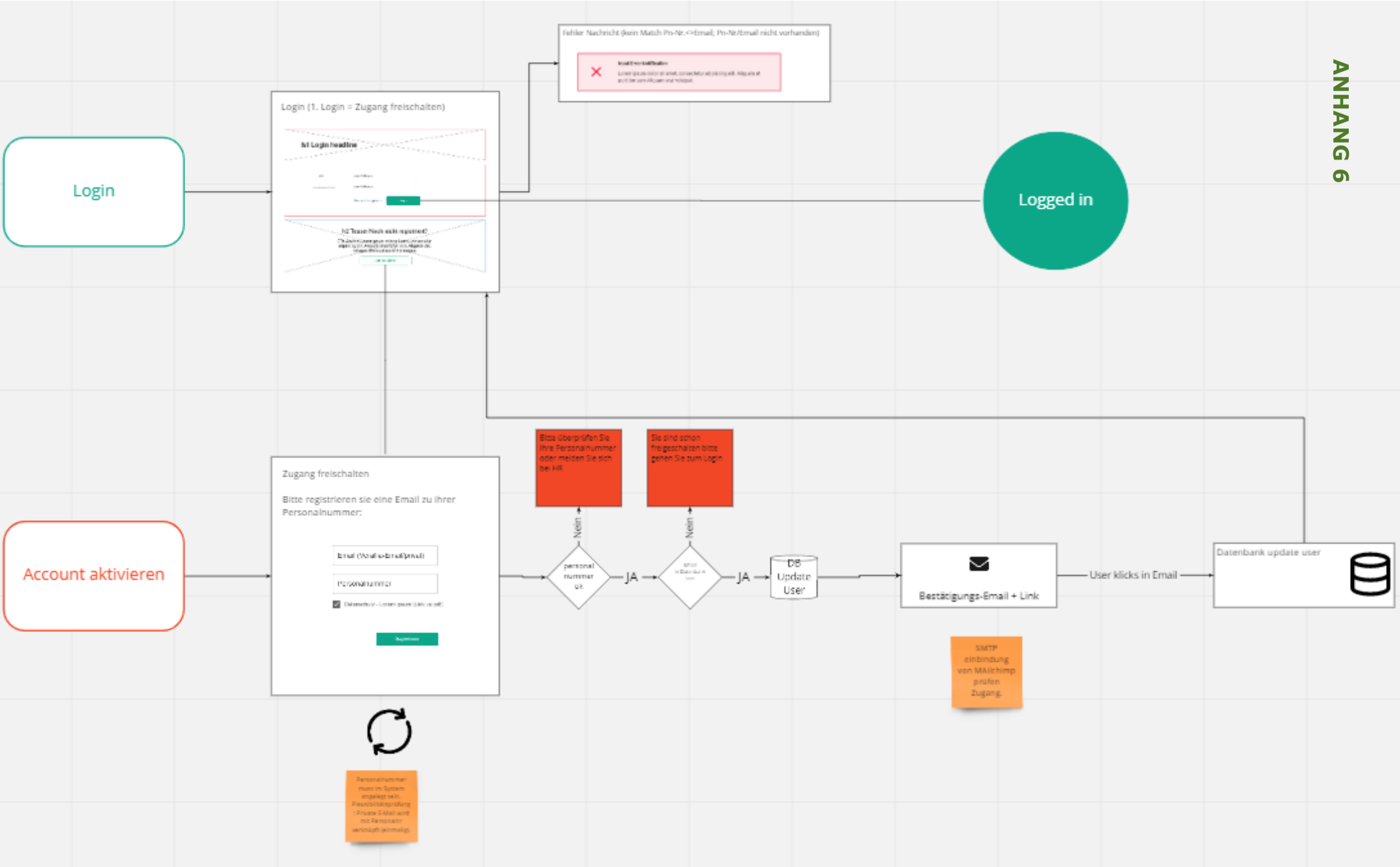
Sie haben es geschafft!

ANHANG 4


verallia
DEUTSCHLAND
Zugang freischalten
E-Mail-Adresse
Personalnummer
Ja, ich habe die Datenschutzerklärung zur Kenntnis genommen und bin damit einverstanden, dass die von mir angegebenen Daten elektronisch erhoben und gespeichert werden.*
Zugang freischalten
Zum Login

ANHANG 5


verallia
DEUTSCHLAND
Herzlich Willkommen!
Bitte melden Sie sich mit Ihren Zugangsdaten an.
E-Mail-Adresse
Personalnummer
Anmelden
Sie haben Ihren Zugang noch nicht freigeschaltet?
Sie müssen Ihren Account bitte einmalig aktivieren, damit der Login möglich ist.
Jetzt Zugang freischalten
Bei Problemen oder Anmerkungen wenden Sie sich bitte an:
loremipsum@dolor.sit


Login
Login (1. Login = Zugang freischalten)
Fehler Nachricht (kein Match Pn-Nr.<>Email; Pn-Nr/Email nicht vorhanden)
Logged in
Account aktivieren
Zugang freischalten
Bitte registrieren sie eine Email zu ihrer Personalnummer:
Bitte überprüfen Sie Ihre Personalnummer oder melden Sie sich bei HR
Sie sind schon freigeschalten bitte gehen Sie zum Login
Nein
Nein
personal nummer ok
JA
JA
DB Update User
Bestätigungs-Email + Link
User klicks in Email
Datenbank update user
SMTP einbindung von Mailchimp prüfen Zugang.