VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN DES VERANTWORTLICHEN (ART 30 ABS. 1 DSGVO)

INHALTSVERZEICHNIS

Eine Übermittlung an Empfänger in einem Drittland (außerhalb der EU) oder an eine internationale Organisation ist nicht vorgesehen. Es besteht keine automatisierte Entscheidung (Profiling).

ANGABEN ZUM VERANTWORTLICHEN (ART. 30 ABS. 1 LIT. A DSGVO)

WELLCON Gesellschaft für Prävention und Arbeitsmedizin GmbH
Invalidenstraße 5
1030 Wien
T: +43/1/218 50 65-311
E: serviceline@wellcon.at
www.wellcon.at

ANGABEN ZUR PERSON DES DATENSCHUTZBEAUFTRAGTEN

Mag. Erwin Leitgeb
T: +43/1/218 50 65-311
E: dsb-wellcon@vaeb.at

Verzeichnis der Verarbeitungstätigkeiten wird laufend aktualisiert.

Bei den nachfolgend verwendeten personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter.

VERARBEITUNGSTÄTIGKEITEN

1. DATENANWENDUNG	KUNDENVERWALTUNG, FINANZBUCHHALTUNG, RECHNUNGSWESEN, LOGISTIK
Zweck der Verarbeitung:	Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung (bzw. zur Abwicklung dieser) mit Kunden und Lieferanten sowie Vertragsverwaltung inklusive Kreditoren- und Debitorenverwaltung, Budgetierung, Kostenrechnung, Einkauf und Logistik einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
Rechtsgrundlage der Verarbeitung:	Die Daten werden auf Basis der zugrunde liegenden Vertragsbeziehungen zwischen dem Verantwortlichen und dem Kunden bzw. Leistungserbringer und auf Basis der bestehenden Rechtsnormen (z.B. BAO, UGB) verarbeitet (Art. 13 (2) lit e). Kontaktdaten von Betroffenen, welche dem Kunden bzw. dem Leistungserbringer zuzurechnen sind (z.B. Mitarbeiter), werden dem Verantwortlichen vom Kunden bzw. Leistungserbringer oder unmittelbar vom Betroffenen mitgeteilt (Art. 14 (2) lit f). Art 6 Abs 1 lit b) iVm Art 6 Abs 1 lit c)
Beschreibung der **Kategorien betroffener Personen**:	Kunden, Lieferanten (Empfänger und Erbringer von Lieferungen oder Leistungen), Sachbearbeiter sowie an der Geschäftsabwicklung mitwirkende Dritte
Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:	siehe Anlage

Datenkategorien und Löschfristen

Daten sind zu löschen, wenn sie nach Ablauf der gesetzlichen Aufbewahrungsfristen (7 Jahre ab 1.1. des Folgejahres in dem die Ansprüche entstanden sind) für die Bearbeitung von Ansprüchen und Anwartschaften im jeweiligen Einzelfall (auch vor dem Hintergrund möglicher Ansprüche von Angehörigen und Hinterbliebenen oder laufender Rechtsstreitigkeiten) nicht mehr benötigt werden.

Nr	Betroffene Personen	Kategorien personenbezogener Daten	Empfänger	Löschfristen
1	Kunden und Lieferanten inkl. Kontaktperson beim Kunden und Lieferanten	Stammdaten inkl. Kontaktinformationen (etwa Ordnungsnummer, Name, Anrede, Geschlecht, Titel, Adresse, Telefonnummer, E-Mail, Fax, UID-Nummer)	1–9,12–13	§ 132 Abs 1 BAO: 7 Jahre §§ 190, 212 UGB: 7 Jahre § 18 Abs 2 USt: 7 Jahre
2		Vertragsdaten (z.B. Zahlungs- und Leistungsverhalten, UID-Nummer, Vertretungsbefugnisse und Kontaktpersonen etc.)	1–9,12	
3		Daten über Buchhaltung und Controlling	1,3,5,13	
4		Verrechnungs- und Zahlungsdaten (z.B. Bankverbindung, Zahlungs-, Stornobedingungen, Bonität, Mahnstufe, Sperrkennzeichen, Kreditinformationen etc.)	1–9,12–13	
5		Registerauszüge (Firmenbuch etc.)	1–8	

6		Gegenstand der Lieferung oder Leistung	3,12
7		Vertragstexte (Angebote, Zusatzvereinbarungen etc.) und Geschäftskorrespondenzen	1–8, 12–13

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (Art 30 Abs 1 lit. d DSGVO)	
1	Banken
2	Rechtsvertreter
3	Wirtschaftstreuhänder, Wirtschaftsprüfer
4	Gerichte
5	Zuständige Verwaltungsbehörden
6	Inkassounternehmen zur Schuldeneintreibung
7	Fremdfinanzierer wie Leasing- oder Factoringunternehmen und Zessionare, sofern die Lieferung oder Leistung auf diese Weise fremdfinanziert wird
8	Vertrags- oder Geschäftspartner, die an der Lieferung oder Leistung mitwirken bzw. mitwirken sollen
9	Versicherungen aus Anlass des Abschlusses eines Versicherungsvertrages über die Lieferung/ Leistung oder des Eintritts des Versicherungsfalls
10	Bundesanstalt „Statistik Österreich“ für die Erstellung der gesetzlich vorgeschriebenen (amtlichen) Statistiken
11	Konzernleitung des Auftraggebers, bei Lieferanten sowie gewerblichen Kunden und Großkunden
12	Kunden (Empfänger von Leistungen)
13	Interne Stellen, soweit sie an der Ausführung des jeweiligen Geschäftsprozesses beteiligt sind (z.B. Personalabteilung, Rechtsabteilung, Buchhaltung, Rechnungswesen, EDV)

2. DATENANWENDUNG	PERSONALVERWALTUNG INKL. BEWERBERMANAGEMENT
Zweck der Verarbeitung:	Verarbeitung und Übermittlung von Daten für für die Personalplanung, Personalanstellung sowie die Personalentwicklung und die damit verbundenen Verarbeitungen und Übermittlungen für Lohn-, Gehalts- und Entgeltverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies aufgrund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglichen Verpflichtungen jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenzen, Bewerbungsschreiben, Dienstzeugnisse, Testergebnisse, Stellenbeschreibungen) in diesen Angelegenheiten.
Rechtsgrundlage der Verarbeitung:	Die Daten werden auf Basis der zugrunde liegenden Arbeitsvertragsbeziehungen und auf Basis der bestehenden Rechtsnormen (z.B. ASchG, Angestelltengesetz, Kollektivvertrag, Arbeitsverfassungsgesetz, Arbeitskräfteüberlassungsgesetz) verarbeitet (Art. 13 (2) lit e). Die Daten von Betroffenen, welche im Rahmen der Zusammenarbeit mit anderen Organisationen verarbeitet werden (z.B. Kontaktdaten), werden dem Verantwortlichen von den jeweiligen Organisationen oder unmittelbar vom Betroffenen mitgeteilt (Art. 14 (2) lit f). Art 6 Abs 1 lit b) iVm Art 6 Abs 1 lit c); für Bewerber: Art 6 Abs 1 lit a) iVm Art 6 Abs 1 lit f)
Beschreibung der **Kategorien betroffener Personen**:	Dienstnehmer, freie Dienstnehmer und andere arbeitnehmerähnliche Beschäftigte (z.B. Praktikanten, Volontäre, Leiharbeitsnehmer, ehemalige Beschäftigte), Bewerber
Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:	siehe Anlage

Datenkategorien und Löschfristen

Allgemein: Bis zur Beendigung der Beziehung mit dem Betroffenen und darüber hinaus solange gesetzliche Aufbewahrungsfristen bestehen oder solange Rechtsansprüche aus dem Arbeitsverhältnis gegenüber dem Arbeitgeber geltend gemacht werden können (Details siehe unten). Private E-Mail-Daten von der betroffenen Person selbst bei Austritt des Dienstnehmers; berufliche E-Mail-Daten spätestens 4 Monate nach Austritt, außer diese werden noch zum Nachweis oder zur Erfüllung der Leistungspflichten des Verantwortlichen benötigt.

Nr	Betroffene Personen	Kategorien personenbezogener Daten	Empfänger	Löschfristen
1	Dienstnehmer (unabhängig von Anstellungsart)	Stammdaten inkl. Kontaktinformationen (etwa Ordnungsnummer, Name, Anrede, Geschlecht, Titel, Adresse, Telefonnummer, E-Mail, Fax, UID-Nummer)	1–5,9,11–13	§ 1478 ABGB: 30 Jahre
2		Sozialversicherungsdaten (Sozialversicherungsnummer, Zuständigkeit für Beitragsverrechnung)	2–5,10–13	§ 68 ASVG: 3 bzw. 5 Jahre
3		Bankverbindungsdaten	1–6, 9–13	§ 1468 ABGB: 3 Jahre
4		Vertragsdaten (Entgelt, Einstufung, Eintritts-/ Austrittsdatum, Berufsgruppe, Arbeitszeitausmaß, etc.)	1–5, 12–13	§ 132 Abs 1 BAO: 7 Jahre

5		Personalverrechnungsdaten (Entgelt, Sonderzahlungen, Zuschläge, Abgaben, Lohnpfändungen)	1–5, 12–13	§ 132 Abs 1 BAO: 7 Jahre
6		Planungs- und Einsatzzeiten (Zeiterfassung, Abwesenheitszeiten)	5,13	GPLA Prüfung § 132 Abs 1 BAO: 7 Jahre
7		Benutzerdaten EDV/ Kommunikation (z.B. Zugangs-/ Login/Protokolldaten, innerbetriebliche Kommunikationsdaten (E-Mail, Telefonnummer, Fax)	13	Beurteilung im Einzelfall
8	Bewerber	Fähigkeiten und Kenntnisse sowie Qualifikationen (etwa Zeugnisse, Lebenslauf, Beurteilungen, Ausbildungen, Sprachkenntnisse)	13	§§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 1 BEinstG: 6 Monate bzw. länger, wenn im Einzelfall vereinbart §§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 1 BEinstG: 6 Monate bzw. länger, wenn im Einzelfall vereinbart
		Stammdaten über den Mitarbeiter inkl. Kontaktinformationen (Name, Geburtsdatum, Familienstand, Staatsbürgerschaft, Adresse, Telefonnummer, E-Mail,)	13	
		Bewertungen des Mitarbeiters (etwa Dienstzeugnisse)	13	
		Informationen zum beruflichen Werdegang	13	
		Lichtbild	13	
		Angaben zur angestrebten Tätigkeit und möglicher Beginn	13	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (Art 30 Abs 1 lit. d DSGVO)

1	Banken
2	Rechtsvertreter
3	Wirtschaftsprüfer und Steuerberater
4	Gerichte
5	Zuständige Verwaltungsbehörden und Finanzbehörden
6	Inkassounternehmen
7	Vertrags- oder Geschäftspartner, die an der Lieferung oder Leistung mitwirken bzw. mitwirken sollen
8	Versicherungen aus Anlass des Abschlusses eines Versicherungsvertrages über die Lieferung/ Leistung oder des Eintritts des Versicherungsfalls
9	Externe Veranstalter für Events und Fortbildungen
10	Vorsorge- und Krankenkassen
11	Arbeitsmarktservice
12	Gesetzliche Interessenvertretungen
13	Interne Stellen, soweit sie an der Ausführung der jeweiligen Geschäftsprozesses beteiligt sind (z.B. Personalabteilung, Rechtsabteilung, Buchhaltung, Rechnungswesen, EDV)

3. DATENANWENDUNG	VERWALTUNG VON BENUTZERKENNZEICHEN SOWIE ZUGANGS- UND ZUTRITTSSYSTEMEN
Zweck der Verarbeitung:	Systemzugriffskontrolle und Verwaltung von Benutzerkennzeichen für die Datenanwendungen des Verantwortlichen sowie die Verwaltung der Zuteilung von Hard- und Software an die Systembenutzer einschließlich automationsunterstützt erstellter und archivierter Textdokumente (z.B. Korrespondenz) in diesen Angelegenheiten. Beinhaltet auch: Zuteilung von Schlüsseln und anderen für den Zutritt notwendigen Systemen.
Rechtsgrundlage der Verarbeitung:	Die Daten werden auf Basis der zugrunde liegenden Arbeitsvertragsbeziehungen und auf Basis der bestehenden Rechtsnormen (z.B. ASchG, Angestelltengesetz, Kollektivvertrag, Betriebsvereinbarungen, Arbeitsverfassungsgesetz, Arbeitskräfteüberlassungsgesetz) verarbeitet (Art. 13 (2) lit e). Die Daten von Betroffenen, welche im Rahmen der Zusammenarbeit mit anderen Organisationen verarbeitet werden (z.B. Kontaktdaten, Remote-Zugriffsberechtigungsumfang), werden dem Verantwortlichen von den jeweiligen Organisationen oder unmittelbar vom Betroffenen mitgeteilt (Art. 14 (2) lit f). Art 6 Abs 1 lit f) iVm Art 32
Beschreibung der **Kategorien betroffener Personen**:	Zugangs- und zutrittsberechtigte Betroffene
Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:	siehe Anlage

Nr	Kategorien personenbezogener Daten	Von Empfängern	Speicherdauer
1	Stammdaten (Name, Titel, Dienstort etc.) inkl. Beziehung des Berechtigten zum Verantwortlichen	1	5 Jahre
2	Benutzerkennzeichen, Passwörter		
3	Zuteilung von Schlüsseln und anderen für den Zutritt notwendigen Systeme		
4	Zugriffs- und Zutrittsrechte (Gültigkeitsdauer, Bereiche, Zeiten)		

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (Art 30 Abs 1 lit. d DSGVO)	
1	Interne Stellen, soweit sie an der Ausführung der jeweiligen Geschäftsprozesses beteiligt sind (z.B. Personalabteilung, Rechtsabteilung, Buchhaltung, Rechnungswesen, EDV)

4. DATENANWENDUNG	MEDIZINISCHE DOKUMENTATION

Zweck der Verarbeitung:		Erfüllung der gesetzlich vorgesehenen Dokumentationsverpflichtung Arbeitsmedizin. Zweck ist die Untersuchung und Behandlung von Probanden (Mitarbeiter), deren Nachvollziehbarkeit sowie die Abrechnung gegenüber den Krankenkassen sowie der Erfüllung der gesetzlichen Dokumentationsverpflichtung. Verwaltung von Probandendaten zur Unterstützung und Dokumentation medizinischer Behandlung sowie zur Verrechnung von Leistungen, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.		
Rechtsgrundlage der Verarbeitung:		Die Daten werden auf Basis der zugrunde liegenden Vertragsbeziehungen und auf Basis der bestehenden gesetzlichen Dokumentationspflichten (z.B. ÄrzteG, ASchG, PsychologenG) verarbeitet (Art 13 (2) lit e) Art 6 Abs 1 lit b) iVm Art 9 Abs 1 lit a), h)		
Beschreibung der **Kategorien betroffener Personen**:		Probanden/Mitarbeiter sowie Bewerber für bestimmte gefahrengeneigte Tätigkeiten; Versicherte, die die angebotenen Leistungen in Anspruch nehmen; sonstige Ärzte		
Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:		siehe Anlage		
Nr	**Betroffene Personen**	**Kategorien personenbezogener Daten**	**Empfänger**	**Speicherdauer**
1	Probanden/ Mitarbeiter sowie Bewerber für bestimmte gefahrengeneigte Tätigkeiten; Versicherte, die die angebotenen Leistungen in Anspruch nehmen	Stammdaten (Vor-, Zuname, Geburtsdatum, Anschrift, Versicherung, Sozialversicherungsnummer, Zuordnung zum Unternehmen inkl. Kontaktdaten (Adresse, Telefonnummer, E-Mail))	1–4	§ 51 Abs 1 ÄrzteG: 30 Jahre
2		Daten zur Organisation (Betriebszugehörigkeit, Sachbearbeiter beim Unternehmen); Planungsdaten (Untersuchungs- und Behandlungstermine, Verwaltung und Vergabe von Untersuchungsterminen)	3, 4	
3		Leistungs-/Abrechnungsdaten (Status der Untersuchungen, Art der medizinischen Leistungen)	3, 4	
4		Daten zur Gesundheit (z.B. Anamnese, Laborbefunde, Arztbriefe, Röntgenbilder, Diagnosen, Notizen zur Krankengeschichte etc.)	2	
5		Ergebnisse der Untersuchungen (z.B. Ergebniscode, Angabe von möglichen Einschränkungen, VGÜ)	1,3, 4	

6		Begehungsprotokolle sowie Gutachten im Zusammenhang mit Erbringung arbeitsmedizinischer Betreuung und Vorsorge wie z.B. arbeitsmedizinische Untersuchungen (Bescheinigung für den Arbeitgeber ohne medizinische Befunde)	3,4	§ 51 Abs 1 ÄrzteG: 30 Jahre

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (Art 30 Abs 1 lit. d DSGVO)	
1	Öffentliche Stellen/Behörden, die Daten aufgrund gesetzlicher Vorschriften erhalten, z.B. Sozialversicherungsträger, Inspektorate
2	Zuweisung an Labore und/oder überweisende Ärzte anderer Fachrichtungen zum Zweck der Einholung und Bereitstellung notwendiger medizinischer Informationen.
3	Zuständige Abteilung des Arbeitgebers
4	Interne Stellen, soweit sie an der Ausführung der jeweiligen Geschäftsprozesses beteiligt sind (z.B. Personalabteilung, Rechtsabteilung, Buchhaltung, Rechnungswesen, EDV)

5. DATENANWENDUNG	DOKUMENTATION IM RAHMEN DES BETRIEBLICHEN GESUNDHEITSMANAGEMENTS
Zweck der Verarbeitung:	Durchführung von Projekten zur Optimierung des Gesundheitsbewusstseins und -verhaltens der Teilnehmer in Ergänzung zu Maßnahmen einer gesundheitsgerechten Arbeitsplatzgestaltung sowie zur Verbesserung und Erhaltung von Gesundheit und Wohlbefinden. Anwendungsfälle: z.B. Arbeitsplatzbegehungen, arbeitspsychologische Beratungen, Anmeldungen zur berufsorientierten Gesundenuntersuchung (BOGU), Maßnahmen der beruflichen Wiedereingliederungen und „train to work“, Evaluierungen psychischer Belastungen, GBZ- und Stressberatungen, Maßnahmen im Projekt „Gesund & Fit“, diverse „Gesundheitsstraßen“ und Aktionstage, Lehrlingsprojekte der ÖBB und VAEB sowie beim PRAEDIAS-Programm der VAEB.
Rechtsgrundlage der Verarbeitung:	Die Daten werden auf Basis der zugrunde liegenden Vertragsbeziehungen und auf Basis der bestehenden gesetzlichen Dokumentationspflichten (z.B. ÄrzteG, ASchG, PsychologenG) verarbeitet (Art 13 (2) lit e) Art 6 Abs 1 lit b) iVm Art 9 Abs 1 lit a), h)
Beschreibung der **Kategorien betroffener Personen**:	Probanden/Mitarbeiter; Versicherte, die die angebotenen Leistungen in Anspruch nehmen
Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:	siehe Anlage

Nr	Betroffene Personen	Kategorien personenbezogener Daten	Empfänger	Speicherdauer
1	Probanden/ Mitarbeiter; Versicherte, die die angebotenen Leistungen in Anspruch nehmen	Stammdaten (Name, Titel, Geburtsdatum, Anschrift, Telefonnummer, E-Mail, Sozialversicherungsnummer, zuständige Krankenkasse)	1–3	§ 51 Abs 1 ÄrzteG: 30 Jahre
		Veranstaltungsdaten (Gesprächs-/ Veranstaltungsdatum/Termin, Gesprächs-/Veranstaltungsort, Anmeldedatum, Laufnummer/ Fallnummer)	1–3	§ 132 Abs 1 BAO: 7 Jahre §§ 190, 212 UGB: 7 Jahre § 18 Abs 2 USt: 7 Jahre
2		Tätigkeitsbezogene Informationen (Arbeitgeber, Angaben zum Dienstverhältnis, Organisationseinheit bzw. Arbeitsstätte, Tätigkeit im Betrieb (Beginn und Ende), Vorgesetzte bzw. Ansprechpersonen, Informationen zur Arbeitsverrichtung, Kontaktdaten, Sicherheits- und Gesundheitsdokumente)	1–3	
3		Allfällige Anmerkungen (Verlaufsdokumentation, Untersuchungskommentar, Teilnehmerzahl)	3	§ 51 Abs 1 ÄrzteG: 30 Jahre

4		Statuserhebung zu Bewegungsapparat (Beweglichkeitswerte, Muskelstatuswerte, Stabilität, Sensomotorik, Symmetrie)	3	§ 51 Abs 1 ÄrzteG: 30 Jahre
5		Statuserhebung Psychologie (Biografie/ Lebensgeschichte, Gesprächsinhalte, Dimensionen psychischer Belastungen)	3	§ 51 Abs 1 ÄrzteG: 30 Jahre
6		Anamnesedaten (z.B. BMI, Gewicht, Größe etc.)	3	§ 51 Abs 1 ÄrzteG: 30 Jahre
7		Messergebnisse (z.B. Blutzucker etc.)	3	§ 51 Abs 1 ÄrzteG: 30 Jahre

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (Art 30 Abs 1 lit. d DSGVO)	
1	Auftraggeber (Arbeitgeber des Probanden)
2	Sozialversicherungsträger
3	Interne Stellen, soweit sie an der Ausführung der jeweiligen Geschäftsprozesses beteiligt sind (z.B. Personalabteilung, Rechtsabteilung, Buchhaltung, Rechnungswesen, EDV)

6. DATENANWENDUNG	MARKETING FÜR EIGENE ZWECKE
Zweck der Verarbeitung:	Verwenden von eigenen Kundendaten für die Geschäftsanbahnung betreffend das eigene Leistungsangebot einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
Rechtsgrundlage der Verarbeitung:	Die Verarbeitung der Daten erfolgt auf Basis der Einwilligung der Betroffenen und zur Wahrung berechtigter Interessen. Art 6 Abs 1 lit a) iVm Art 6 Abs 1 lit f)
Beschreibung der **Kategorien betroffener Personen**:	Kunden, Interessenten
Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:	siehe Anlage

Nr	**Betroffene Personen**	**Kategorien personenbezogener Daten**	**Empfänger**	**Speicherdauer**
1		Stammdaten inkl. Kontaktinformationen (z.B. Adresse, Telefonnummer, E-Mail, Fax, UID-Nummer)	1	bis auf Widerruf
2		Vertragsdaten (Daten über bereits vorhandene Geschäftsbeziehungen)	1	
3		Produktinteressen	1	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (Art 30 Abs 1 lit. d DSGVO)	
1	Interne Stellen, soweit sie an der Ausführung des jeweiligen Geschäftsprozesses/ Geschäftsanbahnungsprozesses beteiligt sind (z.B. Personalabteilung, Rechtsabteilung, Buchhaltung, Rechnungswesen, EDV)

ANLAGE

SETTINGS DER DATENSICHERHEITSMAßNAHMEN

SERVER UND DATENSICHERUNG

Systemüberwachung erfolgt mittels Hardware-Überwachungstools.
Ein Raid-5-Dateisystem ist auf Servern installiert.
Es gibt Backup-Sicherungssoftware mit täglicher Sicherung auf Backup-Server (HDD) sowie Replikation auf NAS.
Sicherungen erfolgen in mehreren Sicherungsgenerationen.
Server stehen in zwei verschlossenen, klimatisierten Räumen.

VERWALTUNG UND ZUGRIFF AUF BETRIEBSDATEN

Alle Betriebsdaten liegen auf den Serverlaufwerken bzw. auf NAS-Systemen.
Keine Speicherung der Betriebsdaten auf den lokalen Arbeitsplatz-Computern.
Ausnahmen sind Notebooks, Laptops und Ultrabooks – diese sind mit einem Kennwort verschlüsselt und somit vor unbefugtem Zugriff geschützt.
Die Windows-Freigaben auf den Servern werden durch Microsoft Active Directory über User-, Gruppen- und Verzeichnisberechtigungen geregelt.

DATENZUGRIFF ÜBER VERKABELUNG, WLAN, INTERNET

In der Zentrale in Wien sind sämtliche Arbeitsplatz-Computer sowie Notebook-, Laptop- und Ultrabook-Docking-Stationen über eine strukturierte Netzwerkverkabelung mit den Servern verbunden. Es existieren drei voneinander unabhängige und vom Netzwerk getrennte WLAN-Netzwerke. Alle drei sind mittels WPA2 Key verschlüsselt. Die Arbeitsplatz-Computer in den Außenstellen St. Pölten, Linz, Salzburg, Innsbruck, Feldkirch, Villach und Graz sind über eine strukturierte Netzwerkverkabelung mit einer eigenen Firewall und damit in weiterer Folge über eine gesicherte VPN-Verbindung mit der Zentrale in Wien verbunden.
Der Internetzugriff ist über eine Cisco-Firewall abgesichert, der Zugriff auf die Server über das Internet kann nur über eine verschlüsselte VPN-Verbindung erfolgen.
Sophos Endpoint Security und Malewarebytes Anti-Maleware sind als Software auf allen Arbeitsplatz Computern sowie Notebooks, Laptops und Ultrabooks für den lokalen Schutz installiert.

MITARBEITERANWEISUNG

Mitarbeiter/innen sind über die Gepflogenheiten im Haus bzgl. Datenverwaltung und Datensicherheit mittels Dienstanweisung unterrichtet.
Die IT-Stabstelle ist das firmeninterne koordinierende Organ.

FIRMENEXTERNE PERSONEN – REINIGUNGSPERSONAL, GÄSTE

Unbefugter Zugriff auf Daten seitens firmenexterner Personen wird mittels der Maßnahmen zur Zugangs-, Datenträger-, Speicher-, Benutzer- sowie Zugriffskontrolle ausgeschlossen.

VERWALTUNG DER KENNWÖRTER UND SCHLÜSSEL ZU DEN VERSPERRBAREN RÄUMEN

Die Schlüssel zu den versperrbaren Räumen (Serverraum) werden im versperrten IT-Büro aufbewahrt.
Kennwörter zur Datenträgerverschlüsselung werden von der IT-Stabstelle verwaltet.

ZUORDNUNG DER DATENSICHERHEITSMAßNAHMEN

VERWEHRUNG DES ZUGANGS ZU VERARBEITUNGSANLAGEN, MIT DENEN DIE VERARBEITUNG DURCHGEFÜHRT WIRD, FÜR UNBEFUGTE (ZUGANGSKONTROLLE)

Firmenräumlichkeiten sind mit Alarmanlage gesichert.
Der Serverraum ist mit einer zusätzlichen Alarmanlage gesichert.
Der Serverraum ist versperrt, Zugang für nicht Berechtigte wird baulich verwehrt.
Das NAS (Network Attached Storage) mit dem externen Sicherungswiederherstellungspunkt steht in einem getrennten Gebäude, der Aufbewahrungsort (Rack im Serverraum) ist mittels Zutrittskontrolle versperrt.
Die Schlüssel befinden sich im versperrten IT-Büro.
Die Zugangscodes für Datenverschlüsselung liegen der IT-Stabstelle vor.

VERHINDERUNG DES UNBEFUGTEN LESENS, KOPIERENS, VERÄNDERNS ODER ENTFERNENS VON DATENTRÄGERN (DATENTRÄGERKONTROLLE)

Die Sicherung auf dem Backup-Server und auf die NAS-Systeme wird mittels AES (Advanced Encryption Standard) 128/256 verschlüsselt.
Eine Anmeldung am Server wird über Active Directory geregelt.
Sophos Endpoint Security und Malewarebytes Anti-Maleware sind als Software auf allen Computern, Notebooks, Laptops, Ultrabooks und Servern für den lokalen Schutz gegen Virenbefall installiert.
Usernamen und Kennwörter zur Datenverschlüsselung liegen der IT-Stabstelle vor.

VERHINDERUNG DER UNBEFUGTEN EINGABE VON PERSONENBEZOGENEN DATEN SOWIE DER UNBEFUGTEN KENNTNISNAHME, VERÄNDERUNG UND LÖSCHUNG VON GESPEICHERTEN PERSONENBEZOGENEN DATEN (SPEICHERKONTROLLE)

Die Absicherung des Zugriffs durch Anmeldung wird über Active Directory mit entsprechenden User- und Gruppenberechtigungen geregelt.
Es werden keine betrieblichen Daten auf den Computern der Arbeitsplätze gespeichert, alle betrieblichen Daten liegen auf den gesicherten Serverlaufwerken.
Notebook-, Laptop- und Ultrabook-Festplatten und/oder SSD werden mittels Kennwort verschlüsselt.
Der Zugriff auf die Betriebsdaten auf den Serverlaufwerken erfolgt über eine im Haus verlegte strukturierte Verkabelung oder über Internet durch eine verschlüsselte VPN-Verbindung – die Zugangsdaten werden durch die IT-Stabstelle verwaltet.
Sicherungsmedien zur Unterbringung außerhalb der Betriebsgebäude (Feuer-, Diebstahls- und Vandalismusgefahr) sind mit AES128/256 verschlüsselt.

VERHINDERUNG DER NUTZUNG AUTOMATISIERTER VERARBEITUNGSSYSTEME MITHILFE VON EINRICHTUNGEN ZUR DATENÜBERTRAGUNG DURCH UNBEFUGTE (BENUTZERKONTROLLE)

Die Absicherung des Zugriffs durch Anmeldung wird über Active Directory mit entsprechenden User- und Gruppenberechtigungen geregelt.
Der Zugriff auf die Betriebsdaten über Internet erfolgt ausschließlich durch eine verschlüsselte VPN-Verbindung.
Schriftliche Aufzeichnungen über die definierten Benutzer- und Gruppenberechtigungen liegen vor.

GEWÄHRLEISTUNG, DASS DIE ZUR BENUTZUNG EINES AUTOMATISIERTEN VERARBEITUNGSSYSTEMS BERECHTIGTEN AUSSCHLIEßLICH ZU DEN IHRER ZUGANGSBERECHTIGUNG UNTERLIEGENDEN PERSONENBEZOGENEN DATEN ZUGANG HABEN (ZUGRIFFSKONTROLLE)

Die Gewährleistung erfolgt über Active Directory durch User- und Gruppenzugriffsbeschränkung und Vergabe von entsprechenden Berechtigungen auf Verzeichnisebene.
Es gibt eine Kennwortvergabe bei Datenbanken und Office-Dateien.

Die Installation und Konfiguration von automatischen Windows-Sicherheits-Updates der einzelnen Arbeitsstationen erfolgt über Deskcenter-Update-Verwaltung.

GEWÄHRLEISTUNG, DASS ÜBERPRÜFT UND FESTGESTELLT WERDEN KANN, AN WELCHE STELLEN PERSONENBEZOGENE DATEN MITHILFE VON EINRICHTUNGEN ZUR DATENÜBERTRAGUNG ÜBERMITTELT ODER ZUR VERFÜGUNG GESTELLT WURDEN ODER WERDEN KÖNNEN (ÜBERTRAGUNGSKONTROLLE)

Die Absicherung des Exchange-Server-E-Mail-Verkehrs ist über Sicherheitszertifikat geregelt.
Eine WELLCON-Dienstanweisung regelt den Umgang mit personenbezogenen Daten.
Es gibt keinen unverschlüsselten Versand von personenbezogenen Daten.
Die Verschlüsselung von Dateianhängen in E-Mails erfolgt mittels der Software 7-Zip.

GEWÄHRLEISTUNG, DASS NACHTRÄGLICH ÜBERPRÜFT UND FESTGESTELLT WERDEN KANN, WELCHE PERSONENBEZOGENEN DATEN ZU WELCHER ZEIT UND VON WEM IN AUTOMATISIERTE VERARBEITUNGSSYSTEME EINGEGEBEN WORDEN SIND (EINGABEKONTROLLE)

Elektronische Eingabe von personenbezogenen Daten wird per Projektplanung dokumentiert.
Standardisierte Eingabemasken befinden sich in Projektordnerstruktur auf gesicherten Netzlaufwerken.
Die Protokollierung der Verwendungsvorgänge erfolgt mittels elektronischer Tätigkeitsaufzeichnung bzw. Protokollvorlagen.

VERHINDERUNG, DASS BEI DER ÜBERMITTLUNG PERSONENBEZOGENER DATEN SOWIE BEIM TRANSPORT VON DATENTRÄGERN DIE DATEN UNBEFUGT GELESEN, KOPIERT, VERÄNDERT ODER GELÖSCHT WERDEN KÖNNEN (TRANSPORTKONTROLLE)

Es gibt eine Active Directory mit Benutzer-, Gruppen- und Verzeichniszugriff.
Es gibt eine Verschlüsselung für Notebook-, Laptop- und Ultrabook-Festplatten (HDD) sowie Solid State Disks (SSD).
Die Verschlüsselung mit AES128/256 der Sicherungsdaten von BackupExec und Veeam Backup sowie auf den NAS-Systemen.
Die Absicherung des Exchange-Server-E-Mail-Verkehrs ist über Sicherheitszertifikat geregelt.

GEWÄHRLEISTUNG, DASS EINGESETZTE SYSTEME IM STÖRFALL WIEDERHERGESTELLT WERDEN KÖNNEN (WIEDERHERSTELLUNG)

Es gibt Raid-5-Festplatten-Systeme bei Servern.
Es gibt ein Backup mit Recovery und Wiederherstellung bis auf Dateiebene-Funktion.
Es gibt eine tägliche Sicherung der gesamten Server-Farm auf Backup-Server sowie Replikation in getrenntem Serverraum mit mehreren Sicherungsgenerationen, die außerhalb der Gebäude gelagert werden können.
Es wird ein täglicher Wiederherstellungspunkt auf externes NAS erstellt.

GEWÄHRLEISTUNG, DASS ALLE FUNKTIONEN DES SYSTEMS ZUR VERFÜGUNG STEHEN, AUFTRETENDE FEHLFUNKTIONEN GEMELDET WERDEN (ZUVERLÄSSIGKEIT) UND GESPEICHERTE PERSONENBEZOGENE DATEN NICHT DURCH FEHLFUNKTIONEN DES SYSTEMS BESCHÄDIGT WERDEN KÖNNEN (DATENINTEGRITÄT)

Es gibt ein Raid-5-Festplatten-System bei Servern sowie ein Überwachungstool für die Server-Farm.
Klimatisierte Serverräume sorgen für optimale Betriebstemperatur.
Die Überwachung erfolgt mittels Temperaturkontrolle.