Anlage 2 –Technisch-organisatorische Maßnahmen

Der Auftragnehmer greift für eine sichere Datenverarbeitung auf die Dienstleistungen verschiedener professioneller Anbieter zurück, die auf die Bereitstellung von Servern und ähnlichen Dienstleistungen spezialisiert sind.

Die nachfolgenden technischen und organisatorischen Maßnahmen des Auftragnehmers setzten sich daher aus zwei Teilbereichen zusammen. Es wird zwischen den Maßnahmen von (Auftragnehmer-Name) sowie der jeweiligen Unterauftragnehmer unterschieden. Dabei werden sowohl die von den Dienstleistern bestimmten Vorgaben als auch die vertraglich vereinbarten Maßnahmen zur Sicherstellung der personenbezogenen Daten berücksichtigt.

1. Technisch Organisatorische Maßnahmen der Unterauftragnehmer

Als verantwortungsvoller Auftragnehmer arbeitet we empower you GmbH mit professionellen Anbietern für Serverdienstleistungen zusammen. Dieser setzt seinen eigenen technischen und organisatorischen Maßnahmen ein. Insbesondere wird hierbei auf die Maßnahmen zur **Sicherstellung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit** der personenbezogenen Daten hingewiesen.

Die personenbezogenen Daten des Auftragnehmers werden im Cloud-basierten CRM-System des Dienstleisters Salesforce gespeichert und bearbeitet. Die Daten werden auf Servern innerhalb der EU gespeichert und verarbeitet. Da sich der Hauptsitz von Salesforce jedoch in den USA befindet, kann eine Übermittlung von Daten in die USA Behörden nicht gänzlich ausgeschlossen werden. Salesforce ist für Nicht-HR-Daten zertifiziert nach dem EU-US-Data Privacy Framework, so dass die Datenübermittlung in diesem Bereich darauf, bzw. den Angemessenheitsbeschluss der EU-Kommission hierzu gestützt wird. Für die HR-Daten ist Rechtsgrundlage die von der EU-Kommission beschlossenen Standardvertragsklauseln, die im Auftragsverarbeitungsvertrag mit Salesforce verarbeitet sind.

Die unten aufgeführten technischen und organisatorischen Maßnahmen von Salesforce) entsprechen dem zum Vertragsabschluss aktuellen Stand MONAT, JAHR.

1.1	Werden personenbezogene Daten der Auftraggeberin auf Servern gespeichert, die von etwaigen Dienstleistern betrieben werden? ☒ ja ☐ nein
1.2	Bei welchem Dienstleister werden die hier verarbeiteten personenbezogenen Daten gespeichert? ☐ Amazon Webservices (AWS) ☐ Heroku (salesforce) ☒ Salesforce ☒ Microsoft Azure
1.3	Unter folgenden Links können auf die zum Zeitpunkt des Vertragsschlusses gewährleisteten technischen und organisatorischen Maßnahmen der eingesetzten Dienste abgerufen werden. - Salesforce: LINK - Microsoft Azure: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14

Die Anmelde- und Zugriffsvoraussetzungen auf die Server der Dienstleister werden durch diese wie folgt administriert:

Authentifizierung gegenüber den Serveranbietern	
2.1.	Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? ☒ ja ☐ nein
2.2	Existieren verbindliche Passwortparameter zur Anmeldung bei den projektbezogenen Softwareanwendungen? ☒ ja ☐ nein Durch wen werden die Parameter vorgegeben: Salesforce
2.3	Passwort-Zeichenlänge: 8 Muss das Passwort Sonderzeichen enthalten? ☒ ja ☐ nein Mindest-Gültigkeitsdauer in Tagen: 30
2.4	Zwingt das IT-System den Nutzer zur Einhaltung der oben genannten PW Vorgaben? ☒ ja ☐ nein
2.5	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? ☒ Admin vergibt neues Initialpasswort ☐ andere, nämlich:
2.6	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? ☒ ja, 3 Versuche ☐ nein
2.7	Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde? ☒ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☐ Die Zugänge bleiben für bitte Wert in Minuten eintragen Minuten gesperrt.

Eine gesicherte Datenübermittlung beim Zugriff auf die Server der Dienstleister wird wie folgt gewährleistet:

Maßnahmen zur sicheren Datenübertragung zwischen den Arbeitsplätzen des Auftragnehmers und den genutzten Servern	
3.1	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? ☐ gar nicht ☐ nein, Datenübertragung erfolgt per MPLS ☐ nur vereinzelt ☐ per verschlüsselter Datei als Mailanhang ☐ per PGP / S/MIME ☐ per verschlüsseltem Datenträger ☐ per VPN ☒ per https/TLS

	☐ per SFTP ☐ Sonstiges: bitte angeben
3.2	Wer verwaltet die Schlüssel bzw. die Zertifikate? ☒ Anwender selbst ☐ eigene IT ☐ Externer Dienstleister
3.3	Werden die Übertragungsvorgänge protokolliert? ☐ ja ☒ nein
3.4	Wie lange werden diese Protokolldaten aufbewahrt? bitte Wert in Tagen eintragen Tage
3.5	Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☒ nein, eine Auswertung wäre aber im Bedarfsfall möglich

2. Technisch organisatorische Maßnahmen des Auftragnehmers

Als Auftragnehmer ergreift der Auftragnehmer die notwendigen **Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität** der ihr anvertrauten personenbezogenen Daten wie folgt:

Zutrittskontrollmaßnahmen zu den Büroräumlichkeiten von (Auftragnehmer-Name)	
1.1	Der **Hauptstandort** des Auftragnehmers befindet sich in (Adresse)
1.2	Der Zutritt zur Büroetage wird kontrolliert und ist grundsätzlich verschlossen.
1.3	Der Zutritt zu den einzelnen Büros ist nur den Geschäftsführern sowie den Projektverantwortlichen möglich. Hierzu werden personalisierte Zugangsberechtigungen benötigt.
1.4	Der Zutritt zu der Büroetage ist über ein **elektronisches Schließsystem** gesichert.
1.5	Zur Authentifizierung benötigen die Mitarbeiter ihr Mobiltelefon sowie die hierauf installierte App des Schließsystemanbieters.
1.6	Die Zutrittsrechte sind für jeden Mitarbeiter personifiziert vergeben. Die elektronischen Schlösser folgen funktional der Unternehmensorganisation.
1.7	Positive Zutrittsversuche werden im Zutrittssystem protokolliert.
1.8	Abgewiesene Zutrittsversuche werden protokolliert.
1.9	Die Protokolle über die Zutritte werden für einen Zeitraum von >30 Tagen aufbewahrt.
1.10	Auswertungen der Protokolle werden im Bedarfsfall vorgenommen.
1.11	Für den Zugang zur Büroebene sowie den einzelnen Büros sind **mechanische Schlösser** eingebaut, welche durch ein **elektronisches Zugangssystem** ergänzt wurden.
1.12	Mobiltelefon wird zur Authentifizierung gegenüber dem elektronischen Zugangssystem benötigt. Dieses muss für den Zugang durch den Besitzer des Mobilgerätes entsperrt werden. Der Besitz des Gerätes ist somit nicht ausreichend.
1.13	Ausschließlich die Geschäftsführung verfügt über die zugangsberechtigten Schlüssel.
1.14	Die Schlüsselausgabe wird protokolliert. Die Ausgabe erfolgt ausschließlich durch die Geschäftsführung.
1.15	Es besteht ein dokumentierter Prozess zur Vergabe der elektronischen Zugangsberechtigungen bzw. zur anlassbezogenen Anpassung der Zutrittsberechtigungen.
1.16	Grundsätzlich werden betriebsfremde Personen werden am Eingang vom Ansprechpartner abgeholt und dürfen sich im Gebäude / Büroetage nur begleitet bewegen.

Unternehmensseitige Zugangs- und Zugriffskontrollmaßnahmen auf projektbezogene Serverdaten	
2.1	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen? ☐ definierter Freigabeprozess ☐ kein definierter Freigabeprozess, auf Zuruf ☐ Sonstige Vergabeweise: bitte angeben
2.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen und Projektbeteiligungen protokolliert? ☐ ja ☐ nein

Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern	
3.1	Papierbasierte Unterlagen mit personenbezogenen Daten verwendet fachgerecht entsorgt. Es stehen hierfür entsprechende Container zur Verfügung in denen papierbasierte Unterlagen entsorgt werden können (Datentonnen). Ein hierauf spezialisierte Entsorgungsdienstleister wird eingesetzt.
3.2	Mobile und externe Datenträger mit personenbezogenen Daten verwendet fachgerecht entsorgt. Es stehen hierfür entsprechende Container zur Verfügung in denen papierbasierte Unterlagen entsorgt werden können (Datentonnen). Ein hierauf spezialisierte Entsorgungsdienstleister wird eingesetzt.
3.3	Grundsätzlich ist der Einsatz von USB-Sticks nicht erlaubt. Lediglich in absoluten Ausnahmefällen und nach vorheriger Absprache und Erlaubnis der Geschäftsführung ist eine entsprechende Anwendung erlaubt. Sofern personenbezogene Daten hierauf gespeichert werden, sind diese nach dem Datentransfer sofort zu löschen. Es werden ausschließlich unternehmenseigene USB-Sticks verwendet. Eine Speicherung erfolgt grundsätzlich verschlüsselt.
3.4	Dürfen die Mitarbeiter private Datenträger (z.B. USB-Sticks) verwenden? ☐ generell ja ☐ ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. ☐ nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.
3.5	Die Speicherung von personenbezogenen Daten auf mobilen Endgeräten erfolgt im ausgeschalteten Modus ausschließlich verschlüsselt.
3.6	Die Verarbeitung von personenbezogenen Daten auf mitarbeitereigenen Geräten ist nicht erlaubt (bring your own device).
3.7	Inaktivität an einem Bildschirm von 10 Minuten führt zu einer automatischen Sperrung des Zuganges und macht eine erneute Anmeldung notwendig.

Administrierung von Mobilgeräten	
4.1	Die durch den Auftraggeber ausgegebenen Mobilgeräte werden nicht durch ein MDM administriert. Sperr- sowie Löschzugriffe sind hierdurch nicht möglich.
4.2	Die Aktualität und Sicherheit der installierten Betriebssysteme auf den Mobilgeräten wird nicht über das MDM gewährleistet.

Verfahren zur Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen	
5.1	Es existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung beim Auftragnehmer.
5.2	Prüfungen erfolgen in regelmäßigen Abständen von 12 Monate .
5.3	Die Prüfergebnisse werden dokumentiert.

Mit den Serverdienstleistern wurde folgende vertragliche Vereinbarungen in Bezug auf **Pseudonymisierung und Verschlüsselung** getroffen:

Vereinbarte Anforderungen an die Serveranbieter, durch (Auftragnehmer-Name) vertraglich festgelegt	
Einsatz von Pseudonymisierung	
6.1	Werden verarbeitete personenbezogene Daten pseudonymisiert? ☐ ja Bitte Kategorien der Daten angeben. ☐ nein
6.2	Werden Algorithmen zur Pseudonymisierung eingesetzt? ☐ ja ☐ nein
6.3	**Wenn ja:** Welcher Algorithmus wird zur Pseudonymisierung eingesetzt? Klicken Sie hier, um Text einzugeben.
6.4	Erfolgt eine Trennung der Zuordnungsdaten und eine Aufbewahrung in getrennten Systemen? ☐ ja ☐ nein
6.5	Wie kann die Pseudonymisierung bei Bedarf Rückgängig gemacht werden? **Mehrfachantworten möglich!** ☐ gemäß einem definierten Verfahren ☐ im Mehr-Augen-Prinzip ☐ Direktzugriff auf nicht pseudonymisierte Rohdaten ☐ Auf Weisung des Vorgesetzten ☐ Sonstiges: bitte eintragen
Einsatz von Verschlüsselung	
7.1	Werden verarbeitete personenbezogene Daten über die bereits beschriebenen Maßnahmen hinaus verschlüsselt? ☐ ja Bitte Kategorien der Daten angeben. ☐ nein
7.2	Welcher Arten der Verschlüsselung werden eingesetzt? **Mehrfachantworten möglich!** Im Fall der Mehrfachantworten beschreiben Sie bitte im Feld „Sonstige“, welche Art der Verschlüsselung für welche Daten eingesetzt wird. ☐ Ende-zu-Ende-Verschlüsselung ☐ Transportverschlüsselung ☐ Data-at-Rest-Verschlüsselung ☐ Sonstige: bitte eintragen.
7.3	Welche kryptographischen Algorithmen werden zur Verschlüsselung oder für verschlüsselungsartige Maßnahmen (z. B. Hashen von Passwörtern) eingesetzt? ☐ AES ☐ SHA-256 ☐ RSA-2048 oder höher ☐ Sonstige: bitte eintragen
7.4	Wer hat Zugriff auf die Verschlüsselten Daten? Mitarbeiter aus den Abteilungen: bitte eintragen. Insgesamt haben … Mitarbeiter Zugriff auf die verschlüsselten Daten
Belastbarkeit	
8.1	Es existieren Maßnahmen, die die Fähigkeit gewährleiten, die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. ☐ nein

	☐ ja bitte Maßnahmen beschreiben.
Wiederherstellbarkeit	
9.1	Existieren Notfall- oder Recoverykonzepte und Maßnahmen über B.2.11 hinaus, die die Fähigkeit gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen? ☐ nein ☐ ja bitte Maßnahmen beschreiben.