Vereinbarung zur Auftragsdatenverarbeitung

gemäß Artikel 28 DSGVO

zwischen der

- Verantwortlicher - nachstehend Auftraggeber genannt **-**

und

PROSTEP AG
Dolivostraße 11
64293 Darmstadt

-Auftragsverarbeiter – nachstehend Auftragnehmer genannt -

PRÄAMBEL

Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden Anwendung auf alle vertraglichen Leistungen der Auftragsverarbeitung, die der Auftragnehmer gegenüber dem Auftraggeber erbringt, und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können (diesbezügliche vertragliche Vereinbarungen im Folgenden nur „Hauptvertrag“ genannt).

GLEICHSTELLUNGSHINWEIS

In folgendem Dokument wird in der Dokumentation respektive für die Beschreibung von Aufgaben, Funktionen oder Rollen aus Vereinfachungsgründen die männliche Schreibweise gewählt. Mit der gewählten Schreibweise werden in diesem Dokument alle Geschlechter angesprochen, denen Aufgaben, Funktionen oder Rollen zugeordnet werden, ohne eine Wertung ihres Geschlechts, ihrer physischen oder psychischen Fähigkeiten, oder eine sonstige Wertung vorzunehmen.

1 LEISTUNGSBESCHREIBUNG

1.1 Der Auftragnehmer verarbeitet im Rahmen des Auftrags für den Auftraggeber personenbezogene Daten für Zwecke der Bereitstellung der im **Anlage 1 (Leistungsbeschreibung)** beschriebenen Dienste des Auftragnehmers. Gegenstand, Dauer des Auftrags, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

1.2 Der Auftraggeber kann den Auftrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will, oder der Auftragnehmer vertragliche oder gesetzlich vorgeschriebene Kontrollmaßnahmen des Auftraggebers vertragswidrig verweigert.

2 TECHNISCH-ORGANISATORISCHE MAßNAHMEN

2.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

2.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. C, Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen (resultierend aus möglichem Verlust, Veränderung, Vernichtung, unbefugtem Zugang oder Offenlegung) im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

2.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

2.4 Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen (mind. in Textform). Werden wesentliche Änderungen der technischen und organisatorischen Maßnahmen vorgenommen, sind diese mit dem Auftraggeber abzustimmen. Die Änderungen sind schriftlich zu fixieren und werden Vertragsbestandteil gemäß der **Anlage 2 (Technische und organisatorische Maßnahmen)**. Einer Abstimmung bedarf es jedoch dann nicht, wenn die Änderungen zu einer Verbesserung des im Rahmen dieser Vereinbarung über eine Datenverarbeitung im Auftrag vereinbarten Datenschutzniveaus führen und der Auftraggeber über diese Änderungen informiert wird; mit Zurverfügungstellung der Informationen werden diese Änderungen automatisch Vertragsbestandteil; **Anlage 2 (Technische und organisatorische Maßnahmen)** ist entsprechend anzupassen.

2.5 Die Verarbeitung von personenbezogenen Daten in Privatwohnungen oder im Rahmen der Telearbeit ist mit dem Auftraggeber in dokumentierter Form abzustimmen. In diesem Zusammenhang steht dem Auftraggeber ein Widerspruchsrecht zu, welches bei Nichtausübung binnen 14 Tagen nach Bereitstellung der Informationen, über die in diesem Absatz betreffende Verarbeitung, als Zustimmung des Auftraggebers zu werten ist. Der Auftragnehmer stellt sicher und sichert zu, dass bei in der Privatwohnung oder in Form von Telearbeit erbrachten Diensten oder Arbeiten die Einhaltung von erforderlichen besonderen Maßnahmen zum Datenschutz im Sinne der Art. 32 DSGVO sichergestellt ist.

3 BERICHTIGUNG, SPERRUNG UND LÖSCHUNG VON DATEN

3.1 Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen, zu sperren oder deren Verarbeitung einzuschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3.2 Soweit die Parteien im Hauptvertrag nicht etwas Abweichendes vereinbart haben, sind Löschkonzepte, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

4 KONTROLLEN UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

4.1 Der Auftragnehmer verpflichtet sich, personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers zu verarbeiten.

4.2 Der Auftragnehmer verpflichtet alle zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit oder stellt sicher, dass sie einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und hat diese vor der Durchführung der Arbeiten mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen. Ziffer 4.1 gilt für diese Personen entsprechend.

4.3 Unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen unterstützt dieser den Auftraggeber nach besten Kräften bei der Einhaltung der Pflichten des Auftraggebers bezüglich der Sicherheit der Verarbeitung, bei der Meldung von Verletzungen des Schutzes personenbezogener Daten gegenüber Aufsichtsbehörden und den betroffenen Personen sowie bei der Datenschutz-Folgenabschätzung und bei einem sich daraus ergebenen Konsultationserfordernis gegenüber Aufsichtsbehörden.

4.4 Der Auftragnehmer unterwirft sich eventuellen Kontrollmaßnahmen der Datenschutzaufsichtsbehörden und wird den Auftraggeber über eine eventuelle Kontrollmaßnahme unverzüglich in Textform informieren, wenn Daten aus dem Auftrag mit dem Auftraggeber betroffen sind. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, unterstütz ihn der Auftragnehmer nach besten Kräften. Die Unterstützungsleistungen umfassen die Informationsbeschaffung und sind nur dann vorzunehmen, wenn sie gesetzlich möglich sind und der Aufwand der Unterstützungsleistungen angemessen ist. Insbesondere besteht keine Kostentragungspflicht seitens des Auftragnehmers.

4.5 Der Auftragnehmer ist verpflichtet, die einschlägigen Vorschriften zur Bestellung des Datenschutzbeauftragten zu beachten. Die Kontaktdaten des Datenschutzbeauftragten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Derzeit ist Datenschutzbeauftragte(r) (Name, Adresse, Kontaktdaten):

Herr Nadi Sönmez, PROSTEP AG, Dolivostr. 11, 64293 Darmstadt
E-Mail: datenschutz@prostep.com, Tel: 06151 9287 316

Ebenso wird dem Auftraggeber ein Wechsel des Datenschutzbeauftragten unverzüglich in Textform mitgeteilt.

4.6 Der Auftragnehmer ist verpflichtet, regelmäßig die technischen und organisatorischen Maßnahmen sowie die internen Prozesse diesbezüglich zu kontrollieren. Der Auftragnehmer gewährleistet die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber.

4.7 Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten.

4.8 Der Auftragnehmer hat den Auftraggeber unverzüglich in Textform zu informieren, falls er der Auffassung ist, dass eine Weisung gegen deutsche oder europäische Datenschutzvorschriften verstößt.

4.9 Der Auftragnehmer unterstützt den Auftraggeber gemäß Art. 28 Abs. 3 Satz 2 Buchst. e) DSGVO unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 12 bis 23 DSGVO genannten Rechte der betroffenen Personen.

5 UNTERAUFTRAGSVERHÄLTNISSE

5.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

5.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragnehmer) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

5.3 Bei dem Einsatz eines Unterauftragnehmers wird der Auftragnehmer einen Vertrag gemäß Art. 28 DSGVO über die Verarbeitung von Daten im Auftrag mit dem Unterauftragnehmer schließen. Der Unterauftrag ist schriftlich zu fixieren. In dem Vertrag sind dem Unterauftragnehmer Datenschutzpflichten aufzuerlegen, die den Festlegungen im Vertrag zwischen dem Auftraggeber und dem Auftragnehmer entsprechen.

5.4 Kommt der weitere Auftragnehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jedes Unterauftragnehmers. Die allgemeinen Vorschriften hinsichtlich des Verhältnisses zwischen dem Auftragnehmer und dem Unterauftragnehmer bleiben unberührt.

5.5 In **Anlage 3 (Unterauftragsverhältnisse)** zu diesem Vertrag werden sämtliche Unterauftragnehmer des Auftragnehmers zum Zeitpunkt des Vertragsschlusses aufgelistet.

5.6 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer ist erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

5.7 Die vertraglich im Anhang 1 vereinbarte Leistung wird ausschließlich in Deutschland und damit in einem Mitgliedstaat der EU oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der zu erbringenden Leistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Textform und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standardschutzklauseln, genehmigte Verhaltensregeln).

5.8 Eine weitere Auslagerung des Unterauftragnehmers an weitere Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers in Textform.

6 KONTROLLRECHTE DES AUFTRAGGEBERS

6.1 Der Auftragnehmer räumt dem Auftraggeber und/oder dessen Bevollmächtigten bezüglich der getroffenen Datenschutz- und Datensicherungsvorkehrungen ein Besichtigungs- und Kontrollrecht (Inspektionsrecht) ein.

6.2 Dieses Inspektionsrecht hat das Ziel, die Einhaltung der dem Auftragnehmer obliegenden Pflichten in dessen Geschäftsbetrieb zu überprüfen. Der Nachweis kann neben Vor-Ort-Kontrollen auch durch unabhängige Prüfberichte und Zertifizierungen sichergestellt werden. Sofern Vor-Ort-Kontrollen durchgeführt werden sollen, sind diese als Stichprobenkontrollen auszugestalten und grundsätzlich rechtzeitig anzumelden. Der Rhythmus der Kontrollen orientiert sich an der Erforderlichkeit. Der Auftragnehmer erteilt dem Auftraggeber ferner alle erforderlichen Auskünfte. Die Ausübung des Inspektionsrechts darf den Geschäftsbetrieb nicht unangemessen stören oder missbräuchlich sein.

6.3 Es erfolgt keine Kostenerstattung durch den Auftraggeber für durchgeführte Kontrollen bzgl. des Datenschutzniveaus beim Auftragnehmer.

7 MITTEILUNG BEI VERSTÖßEN DES AUFTRAGNEHMERS

7.1 Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich, spätestens jedoch binnen 24 Stunden in Textform zu benachrichtigen, wenn ein begründeter Verdacht einer Verletzung von in diesem Vertrag festgelegten Datenschutz- und Datensicherheitsbestimmungen durch den Auftragnehmer selbst oder durch von ihm beauftragte Dritte besteht. Das gleiche gilt bei Verstößen gegen die allgemeinen Vorschriften zum Schutz personenbezogener Daten.

7.2 Der Auftragnehmer stellt unverzüglich, spätestens jedoch binnen 36 Stunden nach Bekanntwerden einer Verletzung des Schutzes von personenbezogener Daten dem Auftraggeber ausreichend Informationen zur Verfügung, damit der Auftraggeber seiner Pflicht zur Meldung an die zuständige Behörde und die Unterrichtung des Betroffenen nachkommen kann. Der Auftragnehmer ist nicht berechtigt den Betroffenen über die Verletzung des Schutzes von personenbezogenen Daten zu benachrichtigen. Der Auftragnehmer arbeitet mit dem Auftraggeber zusammen und ergreift angemessene geschäftliche Schritte, um den Auftraggeber bei der Untersuchung, Minderung und Beseitigung jeden solchen Verstoßes gegen personenbezogene Daten, bei Datenschutz-Folgeabschätzungen und im Rahmen der vorherigen Konsultation einer Aufsichtsbehörde zu unterstützen.

8 WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

8.1 Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

8.2 Falls der Auftragnehmer eine Weisung nicht einhalten kann, verpflichtet er sich, den Auftraggeber unverzüglich davon in Textform in Kenntnis zu setzen. Der Auftraggeber ist in diesem Fall berechtigt, die Datenweitergabe auszusetzen und/oder von diesem

Vertrag und vom Hauptvertrag, zu dem dieser Vertrag geschlossen wurde, zurückzutreten.

8.3 Mündliche Weisungen wird der Auftraggeber unverzüglich in Textform bestätigen.

8.4 Der Auftragnehmer wird den Auftraggeber unverzüglich in Textform darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen Vorschriften über den Datenschutz verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber in Textform bestätigt oder geändert wird.

9 LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

9.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

9.2 Nach Abschluss der Arbeiten beziehungsweise früher nach Aufforderung durch den Auftraggeber oder bei Beendigung oder Kündigung dieses Vertrages hat der Auftragnehmer sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung durch den Auftraggeber in Textform datenschutzgerecht zu vernichten. Die Datenlöschung und Datenvernichtung muss vollständig und nach anerkannten, dem Stand der Technik entsprechenden Verfahren zum mehrfachen Überschreiben von Daten vorgenommen werden. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Das Protokoll der Löschung ist dem Auftraggeber auf Anforderung vorzulegen und es ist ihm eine Kopie auszuhändigen.

9.2 Eine Datenlöschung und -vernichtung unterbleibt, soweit und solange der Auftragnehmer die Daten im Einzelfall für berechtigte eigene Zwecke, insbesondere zur Dokumentation des Nachweises der auftrags- und ordnungsgemäßen Datenverarbeitung benötigt (beispielsweise die Rechnungsstellung an den Auftraggeber), oder soweit und solange der Auftragnehmer aufgrund gesetzlicher Vorgabe oder behördlicher Anordnung zur Speicherung verpflichtet ist.

10 SONSTIGE REGELUNGEN

10.1 Sollte die auftragsgemäße Erfüllung des Auftragsgegenstandes gemäß Ziffer 1 dieser Vereinbarung beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder ein Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, informiert der Auftragnehmer den Verantwortlichen unverzüglich. Der Auftragnehmer wird alle in diesem Zusammenhang Beteiligte unverzüglich darüber informieren, dass die Verfügungsbefugnisse an den Daten ausschließlich beim Verantwortlichen liegen.

10.2 Bei etwaigen Widersprüchen zwischen diesem Vertrag und einem Hauptvertrag gehen die Regelungen dieses Vertrags den Regelungen des Hauptvertrags vor.

10.3 Sollten einzelne Teile dieses Auftrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

10.4 Jede Veränderung dieser Vereinbarung einschließlich ihrer Kündigung und dieser Klausel bedarf der Schriftform, was auch in einem elektronischen Format erfolgen kann.

UNTERSCHRIFTEN

Für den Auftraggeber:

Darmstadt, den

_____

(Unterschrift)

_____

(Name in Druckschrift)

_____

(Rolle / Position)

Für den Auftragnehmer:

Darmstadt, den

_____

(Unterschrift)

Dr. Bernd Pätzold

(Name in Druckschrift)

Vorsitzender des Vorstands

(Rolle / Position)

ANLAGE 1 – LEISTUNGSBESCHREIBUNG

1. GEGENSTAND UND DAUER DES AUFTRAGS

(1) GEGENSTAND

☒ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
Gegenstand des Auftrags ist die Leistung, die im Angebotsschreiben für den GlobalX SaaS Leistungsumfang definiert ist. Bezogen auf die EU-DSGVO ist hier besonders darauf hinzuweisen, dass die Einrichtung und Pflege von Anwendern und Datenaustauschpartnern (Verarbeitung von personenbezogenen Daten) durch den Kunden selbst erfolgt. PROSTEP ist für den Betrieb der Systeme verantwortlich und leistet im Rahmen dieser Aufgabe im Bedarfsfall 2nd Level Support. In diesem Zusammenhang haben die Mitarbeiter des PROSTEP Produkt Supports Zugriff auf die Anwendungen und können die personenbezogenen Daten einsehen und im Bedarfsfall bearbeiten.

(2) DAUER

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. KONKRETISIERUNG DES AUFTRAGSINHALTS

(1) ART UND ZWECK DER VORGESEHEHEN VERARBEITUNG VON DATEN

☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:
Im Kontext der IT-Systemadministration und des 2nd Level Supports kann es notwendig sein auf Daten aus OpenDXM GlobalX und der dazugehörenden Oracle Datenbank zuzugreifen, aus denen personenbezogene Daten der im System eingerichteten Anwender und Datenaustauschpartner ersichtlich sind. Hierbei handelt es sich um personenbezogene Daten in Form von Benutzerdaten, welche bei der Nutzung von Datenaustauschprozessen anfallen, wie zum Beispiel Vorname, Name, Abteilung/Gruppe, Firmenzugehörigkeit, Telefonnummern (geschäftlich), E-Mailadresse (geschäftlich), ggf. ENGDAT Routing Adressen, Rollenzuordnung, Arbeitsort, Nutzungsverhalten, Zeitstempel in Logdateien, Zuordnung der versendeten und empfangenen Nutzdaten, etc.

(2) ART DER DATEN

☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Kundenhistorie

- ☒ Datentransferhistorie (z.B. Datenbank, Logdateien)
- ☒ Hotline- und Supportanfragen
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Klicken Sie hier, um Text einzugeben

(3) KATEGORIEN BETROFFENER PERSONEN

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☒ Datenaustauschpartner des Auftraggebers
- ☐ Interessenten
- ☒ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☒ Ansprechpartner
- ☐ Klicken Sie hier, um Text einzugeben

ANLAGE 2 – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Unter Berücksichtigung des

- Stands der Technik,
- Der Implementierungskosten und
- der Art, des Umfangs, der Umstände und
- der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

trifft der Auftragnehmer geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Der Auftragnehmer ergreift folgende Maßnahmen:

1. Maßnahmen zur Zutrittskontrolle

Maßnahmen	**Beschreibung**
Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde)	Es besteht eine klare Regelung zu befugten Personen. Der Zutritt erfolgt berechtigungsspezifisch. Der Zutritt zum Unternehmensgebäude erfolgt per (persönlichem) Transponder. Innerhalb des Gebäudes ist der Zutritt zu Bereichen mit erhöhtem Sicherheitsbedarf (IT-Administration) mit zusätzlichen Berechtigungsebenen gesichert. Die Vergabe von Zutrittsberechtigungen erfolgt ausschließlich unter Berücksichtigung der Aufgabenbereiche der Mitarbeiter.
Besucherregelung	Besucher müssen sich beim Empfang anmelden. Es erfolgt eine Abholung am Empfang. Besucher werden stets durch Mitarbeiter auf dem Betriebsgelände begleitet. Die Begleitung erfolgt nach dem Besuch bis zum Ausgang.
Erfassung / Kenntlichmachung von Besuchern	Die Erfassung der Besucher wird am Empfang vor Ort sichergestellt. Besucher erhalten einen offen zu tragenden Besucherausweis.
Schlüsselregelung	Sämtliche Transponder und Schlüssel sind in einer tagesaktuellen Schlüsselliste dokumentiert.

2. Maßnahmen zur Zugangskontrolle

Maßnahmen	**Beschreibung**
Antrag zur Vergabe von Benutzer-Accounts	Die Freigabe zur Einrichtung bzw. Anpassung von Benutzerkonten geschieht nach Durchlauf eines Prüfungs- und Genehmigungsprozesses.
Absicherung der DV-Systeme durch Login-Prozedur	Der Zugang ist passwortgeschützt und die Zugangsdaten nur ausgewählten Mitarbeitern bekannt.
Passwortrichtlinie (bzgl. Länge, Änderungsintervall, etc.)	mindestens 11 Zeichen Groß-/Kleinschreibung, Zahlen, Sonderzeichen 3 der 4 Kriterien müssen erfüllt sein Min. Passwortalter: 1 Tag Max. Passwortalter: 180 Tage Richtlinien und Vorgaben für die Passwortsicherheit sind vorhanden und werden automatisch geprüft.
Sicherungsmaßnahmen bei Verlassen des Arbeitsplatzes	Beim Verlassen des Arbeitsplatzes wird der Rechner vom Benutzer gesperrt. Zusätzlich wird nach 10 Minuten Inaktivität, der Rechner gesperrt.
Passwortsperrung nach mehrmaligen Fehlversuchen	Fehlgeschlagene Anmeldungen werden protokolliert. Mitarbeiter-PCs werden nach mehrmaliger Falscheingabe des Passwortes automatisch gesperrt. Die Sperre erfolgt nach 3-maliger Falscheingabe.
Regelungen / Voraussetzungen zur Telearbeit	Innerhalb des Auftragsverhältnisses erfolgt die Einrichtung von Telearbeitsplätzen nur mit Zustimmung des Auftraggebers.
Absicherung der Netzwerkverbindung bei Telearbeit (z.B. VPN, Zugangstoken)	Soweit Telearbeitsplätze mit Zustimmung des Auftraggebers eingerichtet werden, wird der Zugang durch eine VPN Verbindung mit OTP geschützt.
Einrichtung eines Benutzerstammsatzes pro User (keine Gruppen-Accounts)	Alle Personen / Mitarbeiter erhalten ihr eigenes Benutzerkonto.
Verwahrung von Daten und Dokumenten	Digitale Daten befinden sich auf gesicherten Systemen. Nicht digitale Daten/Dokumente lagern in verschlossenen Schränken / Behältnissen. Aus dem Produktionsprozess herausgelöste Datenträger werden durch zertifizierte Entsorgungsunternehmen datenschutzgerecht entsorgt.

	Der Einsatz von USB-Speichern ist nur verschlüsselt und auf PROSTEP-eigener Hardware gestattet. Der Verlust mobiler Geräte (z.B. durch Aufbruch eines Firmen-Wagens) ist unverzüglich anzuzeigen. Diese Geräte werden für den Zugang zu internen Netzen unverzüglich gesperrt.

3. Maßnahmen zur Zugriffkontrolle

Maßnahmen	**Beschreibung**
Zentrale Vergabestelle von Benutzerrechten	Die Vergabe von Rechten erfolgt sowohl für Kunden, als auch Mitarbeiter über zentrale Systeme.
Formales Antrags- und Genehmigungsverfahren	Der Umfang der Berechtigungen ist abhängig von der Arbeitsplatz-/Tätigkeitsbeschreibung des Mitarbeiters. Mitarbeiter können selbständig keine Rechte einrichten. Die Erweiterung von Rechten ist stets durch den Abteilungsleiter bei der IT-Administration zu genehmigen. Bei Ausscheiden eines Mitarbeiters wird die IT-Administration unverzüglich durch die Personalabteilung informiert. Zum Ausscheidungszeitpunkt werden die Berechtigungen aufgehoben und ggf. eingerichtete Zugänge gelöscht.
Regelung der Zugriffsberechtigung auf Basis definierter Rollen, nicht personengebunden	Der Zugriff auf verschiedene Dienste bzw. Systeme ist durch Gruppenrichtlinien geregelt. Diese werden zentral gesteuert. Ausgangspunkt ist die Arbeitsplatzbeschreibung des Mitarbeiters. Ausschließlich erforderliche Rechte werden über den Abteilungsleiter bei der IT-Administration angefordert.
Ständige Aktualisierung der Zugriffsrechte sowie anlassbezogene Anpassung z.B. beim Abteilungswechsel eines Mitarbeiters innerhalb der Organisation	Es ist organisatorisch geregelt, dass die Rechte der Mitarbeiter bei Änderung ihrer Zuständigkeiten entsprechend angepasst werden.
Zeitliche Begrenzung der Zugriffsmöglichkeiten	Mitarbeiter erhalten nur solange Zugriff auf die entsprechenden Daten, wie dieser für die jeweiligen Aufgaben benötigt wird.
Richtlinien für die Dateiorganisation	Es existieren Vorgaben zur Ablage bzw. Speicherung der Daten bzw. Information durch Mitarbeiter. Die Mitarbeiter nutzen im Rahmen der ihnen eingeräumten Berechtigungen ausschließlich zur Nutzung durch die Unternehmensleitung

	freigegebene Software. Die Datenspeicherung innerhalb der eingesetzten Software wird durch die Datenbankstruktur und die eingeräumten Rechte bestimmt. Laufwerksfreigaben/Ordnerfreigaben werden nur auf Anforderung durch Abteilungsleiter eingerichtet. Auf Daten im Intranet haben nur die Mitarbeiter einen schreibenden Zugriff, die zur Datenpflege legitimiert sind. Alle Mitarbeiter sind für ihre Arbeitsbereiche hinsichtlich der eingesetzten Software und den vorhandenen Speichermöglichkeiten unterrichtet/geschult.
Firewall	Alle Systeme und Netzabschnitte sind durchgehend durch Firewallsysteme geschützt.

4. Maßnahmen zur Weitergabekontrolle

Maßnahmen	**Beschreibung**
Verschlüsselung bei der Datenübermittlung	Datenübertragungen erfolgen immer wenn möglich verschlüsselt.
Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger und Informationen	Datenträger werden physisch zerstört. Die Löschung von Daten erfolgt nach Ablauf der gesetzlichen oder vertraglichen Nachweis- und Aufbewahrungspflichten.
Dokumentation der Abruf- und Übermittlungsprogramme	Die eingesetzten Programme sind alle sowohl für die Mitarbeiter, als auch Kunden dokumentiert.
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der genutzten Übermittlungswege (Konfiguration)	Alle Übermittlungsverfahren sind dokumentiert. Mobile Datenträger werden nicht eingesetzt. Kuriere kommen deshalb nicht zum Einsatz.
Bestimmte autorisierte Benutzer	Es gibt autorisierte Benutzer für verschiedene Arbeitsbereiche, welche spezielle Rechte in Hinsicht auf personenbezogene Daten haben, da diese für die normale Arbeit oder die Fehlersuche benötigt werden.
Fernwartungskonzept	Art, Umfang und Befugnisse für die Fernwartung sind dokumentiert und werden über Managementtools umgesetzt. Der Zugriff auf die Systeme des Auftraggebers kann Webbasiert erfolgen. Dies gilt für Auftragnehmer und Auftraggeber gleichermaßen. Auf Wunsch kann der Zugriff durch den

	Auftragnehmer stets telefonisch angekündigt/genehmigt werden.

5. Maßnahmen zur Eingabekontrolle

Maßnahmen	**Beschreibung**
Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe	Die Berechtigung für die Eingabe/Verarbeitung von Daten durch zuständige Personen ist geregelt.
Verfahrens-, Programm- und Arbeitsablauforganisation	Für alle relevanten Tätigkeiten gibt es grundlegende Dokumentationen.
Authentizität	Bei Bedarf kann über entsprechende Logs eingesehen werden, wann welcher Nutzer Daten angelegt, bearbeitet oder gelöscht hat. Die Identifizierung der Nutzer wird durch die Authentifizierung bei der Anmeldung sichergestellt.

6. Maßnahmen zur Auftragskontrolle

Maßnahmen	**Beschreibung**
Auswahl der (Unter-)Auftragnehmer	Die Auswahl der Auftragnehmer erfolgt unter sorgfältiger Prüfung dessen datenschutzrechtlicher Zuverlässigkeit. Die Prüfung der durch einen Unterauftragnehmer ergriffenen Maßnahmen auf ihre datenschutzrechtliche Geeignetheit erfolgt durch den Datenschutzbeauftragten des Auftragnehmers.
Regelmäßige Kontrolle der Einhaltung datenschutzrechtlicher Vorgaben beim Auftragnehmer	Eine Kontrolle durch den Auftraggeber (z.B. per Begehung durch einen Sachverständigen) ist nach vorheriger Anmeldung jederzeit möglich. Im konkreten Fall erfolgt mangels Unterbeauftragung keine Kontrolle von Unterauftragnehmern.

7. Maßnahmen zur Verfügbarkeitskontrolle

Maßnahmen	**Beschreibung**
Backup	Es existiert ein aktuelles Backupkonzept für das Rechenzentrum des Auftragnehmers. Das Backup erfolgt als Disaster Recovery-Backup, und als 12-wöchiges Archivierungsbackup Alle Infrastruktur-VMs werden zusätzlich einmal

	täglich gesichert. Diese Sicherung wird 3 Tage aufbewahrt. Die Sicherung der VMs ist unabhängig von den Anwendungen, die innerhalb der VM laufen. Die Wiederherstellung aus dieser Sicherung erfolgt immer als vollständige VM.
Reaktionen im Notfall	Es existiert ein aktuelles Notfallkonzept für das Rechenzentrum des Auftragnehmers. Das Notfallkonzept beinhaltet die Information des Datenschutzbeauftragten. Im weiteren Verlauf stellt der Datenschutzbeauftragte im Rahmen seiner Verantwortlichkeit und unter Berücksichtigung der gesetzlichen Anforderungen die Information des Auftraggebers und ggf. der Aufsichtsbörden mit Zustimmung des Auftraggebers sicher.
Absicherungen im Rechenzentrum	– Elektronische und mechanische Zugangskontrollsysteme – Videoüberwachung und Rauchmelder innerhalb des Rechenzentrums – Brandbekämpfungseinrichtungen – Klimatisierung über 2 getrennte Kühlkreisläufe (n+1) – redundante Stromzuführung – unterbrechungsfreie und gefilterte Stromversorgung durch USV-Batterien (Online USV)
Patchmanagement	Das Patchmanagement der Umgebung erfolgt regelmäßig in Abhängigkeit der von Microsoft bereitgestellten Patches und Fixes. Die Auftragnehmerin behält sich vor, einzelne Patches oder größere Servicepacks erst mit angemessener Verzögerung zu installieren, um ggfs. Erfahrungswerte im Hinblick auf die Systemstabilität zu sammeln.
Virenschutz	Zentrale Komponenten, sowie auch alle Mitarbeitersysteme werden vor Viren geschützt. Ein Virenschutzkonzept ist als Bestandteil des Betriebshandbuchs vorhanden und umgesetzt.
Firewall	Zentrale Komponenten, sowie auch alle Mitarbeitersysteme werden vor Angriffen von außen geschützt. Ein Firewallkonzept ist als Bestandteil des Betriebshandbuchs vorhanden und umgesetzt.

8. Maßnahmen zum Trennungsgebot

Maßnahmen	**Beschreibung**
Mandantentrennung	Werden Daten der Auftraggeberin auf den Systemen der Auftragnehmerin gespeichert, werden diese logisch getrennt verarbeitet.
Funktionstrennungen	Die Funktionstrennung gemäß Ziff. 8 der Anlage u § 9 Satz 1 BDSG ist gegeben. Die verschiedenen organisatorischen Bereiche der Auftragnehmerin (wie Entwicklung und Support) erhalten nur Zugriff auf die für ihre Aufgaben relevanten Daten.

ANLAGE 3 – UNTERAUFTRAGSVERHÄLTNISSE

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragsnehmer“).

Name und Anschrift der Unterauftragsnehmer	Gegenstand der Unterbeauftragung	Datum des Vertrags zur Unterbeauftragung
DARZ GmbH *Julius-Reiber-Straße 11* *64293 Darmstadt*	*Bereitstellung der Open DXM GlobalX SaaS Infrastruktur im Hochsicherheitsrechenzentrum*	*17.09.2018*

Bitte senden Sie diese Vereinbarung unterschrieben in zweifacher Ausfertigung an:

PROSTEP AG
z.H. Sabine Kölsch
Dolivostr. 11
64293 Darmstadt

Wir senden Ihnen umgehend ein von uns gegengezeichnetes Exemplar zurück.