Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

[Stand: Januar 2018]

Vereinbarung

zwischen dem/der

Firma: _____

Straße: _____

PLZ / Ort_____

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

CSW Peripheriesysteme GmbH

Herrenpfad-Süd 18

41334 Nettetal

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Vertreter gemäß Art. 27 DS-GVO:

Peter Vroomen / Michael Schepers

Präambel

Diese Vereinbarung berücksichtigt die mit Inkrafttreten der EU-Datenschutzgrundverordnung (EU-DSGVO) sowie das Bundesdatenschutzgesetz in der vom Deutschen Bundestag am 27. April 2017 und dem Deutschen Bundesrat am 12. Mai 2017 beschlossenen Fassung (BDSG-neu) geltende Rechtslage.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung gemäß Wartungsvertrag _____, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung genannt).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Neuinstallation der ProForma Software (Definition der Aufgaben)

(2) Dauer

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

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:
- Erbringung von Supportleistungen der ProForma Software.
- Installation der ProForma Software

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Art der Daten

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

- ☐ Personenstammdaten
- ☐ Personaldaten, die für den Druck der Entgeltabrechnung, Steuerbescheinigung und Meldung zur Sozialversicherung unter Beachtung der Entgeltbescheinigungsverordnung, erforderlich sind.
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten

- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ .....

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ .....

3. Technisch-organisatorische Maßnahmen

(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) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(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. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

   ☒ Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Stefan Kleinermann, Max-Planck-Str. 9, 52499 Baesweiler bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. 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.
f) 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, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der Betroffenen Person gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Auslagerung auf Unterauftragnehmer sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der Geschäftszeiten zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer interne und externe Vergütungsansprüche geltend machen.

8 Fernzugriff bei Prüfung/Wartung eines Systems oder anderen Dienstleistungen über Fernzugriffe

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

(1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt. Der Auftraggeber überwacht den Zugriff.

(2) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.

(3) Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.

(4) Vor Durchführung von Fernzugriffen werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(5) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden auf Anforderung von der Anwendung dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

(6) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

(7) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) des Auftraggebers notwendig ist, erteilt der Auftraggeber vorher die Einwilligung.

(8) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, erteilt der Auftraggeber die vorherige Einwilligung. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchem des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.

(9) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

(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.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

_____ CSW Peripheriesysteme GmbH

_____, den Nettetal, den

Anlage 1

Technische und organisatorische Maßnahmen

nach Art. 32 DS-GVO, § 64 BDSG-NEU

CSW Peripheriesysteme GmbH

1. Vertraulichkeit und Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Zugangskontrolle, § 64 Abs. 3 Nr. 1 BDSG-NEU

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

Benutzer

- An- und Abmeldeprozedur mit Passwortverwaltung
- Personalisierte Adminzugänge
- Festlegung zum Schutz unbeaufsichtigter Systeme, Test- und Produktivsysteme
- Regelung zum Entzug von Zugangsrechten und Zertifikaten bei Beendigung des Dienstverhältnisses oder internem Wechsel

Netze

- Absicherung Zugang zu den Kommunikationsstrukturen aus dem Internet durch starke Authentisierungsmechanismen
- Regelungen zur Zugangsbeschränkung auf nur notwendige Systeme
- Regelungen zu Gruppentrennung und Nutzung von gemeinsamen Netzen
- Konzept zur Absicherung der Netze (Firewall etc.)
- Regelungen zur Authentisierung bei Fernzugriffen
- Festlegungen zur Nutzung und Gestaltung WLAN

Betriebssysteme

- Sicheres Anmeldeverfahren mit sicheren Passwörtern
- Eindeutige Benutzerkennung
- Einschränkung und Überwachung der Nutzung von Admindiensten

Anwendungen

- Regelungen zur Isolierung sensibler Systeme
- Vergabe und Überwachung der Zugänge durch Produktverantwortliche

Fernzugang

- Vorgaben zur Einrichtung eines Remotezugangs
- Befristeter Zugang (Zertifikat)
- Verpflichtung Externer

Systeme generell

- Auditprotokolle sofern durch System unterstützt

Zutritt zum Gelände

- Einfriedung mit Rolltor

Zutritt zum Gebäude

- Elektronisches Schließsystem mit Protokollierung
- Zutritt Externer nur über Eingang Empfang / Registrierung
- Alarmanlage
- Videoüberwachung

Zutritt zu den Büros

- Externe ab Empfang nur in Begleitung eines MA
- Kennzeichnung Externe durch Besucherausweise

Zutritt zu den Rechenzentren

- Protokollierung
- Elektronisches Schließsystem mit Protokollierung

Überprüfung

- Regelmäßige Überprüfung durch die Personalverantwortlichen (Geschäftsführung)
- Regelmäßiges Audit mit Datenschutzbeauftragten
- Schutz gegen unbefugten Zutritt

Datenträgerkontrolle, § 64 Abs. 3 Nr. 2 BDSG-NEU

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern,

Berechtigungen

- Prozess zur Vergabe , Entzug und Kontrolle von Berechtigungen (Genehmigung, Freigabe und
- regelmäßige Überprüfung durch Personalverantwortlichen)
- Vergabe, Überwachung und Dokumentation produktbezogener Berechtigungen durch Produktverantwortlichen

Speicherkontrolle, § 64 Abs. 3 Nr. 3 BDSG-NEU

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten,

- Protokollierung in der jeweiligen Anwendung je nach Weisung des Auftraggebers

Benutzerkontrolle, § 64 Abs. 3 Nr. 4 BDSG-NEU

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

- An- und Abmeldeprozedur mit Passwortverwaltung
- Personalisierte Adminzugänge
- Festlegung zum Schutz unbeaufsichtigter Systeme, Test- und Produktivsysteme
- Regelung zum Entzug von Zugangsrechten und Zertifikaten bei Beendigung des Dienstverhältnisses oder internem Wechsel

Zugriffskontrolle, § 64 Abs. 3 Nr. 5 BDSG-NEU

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

Berechtigungen

- Prozess zur Vergabe , Entzug und Kontrolle von Berechtigungen (Genehmigung, Freigabe und
- regelmäßige Überprüfung durch Personalverantwortlichen)
- Vergabe, Überwachung und Dokumentation produktbezogener Berechtigungen durch Produktverantwortlichen

Clear Desk

- Regelungen zum Schutz der Systeme/Informationen vor unbefugtem Zugriff Dritter
- Automatisierte Sperre
- Zugriff durch Externe nur im Beisein eines MA

Geheimhaltung

- Verpflichtung aller Mitarbeiter auf BDSG TKG und UWG bei Einstellung
- Regelmäßige Wiederholung dieser Verpflichtung
- Verpflichtung aller Externen, die Zugang zu unseren Systemen erhalten (vor Ort oder Remote)
- Regelmäßige Unterweisung aller Mitarbeiter

Mitnahme von Systemen

- Regelung zur Mitnahme von Systemen und Sicherung dieser unterwegs und zuhause
- Kein Speichern von schützenswerten Daten auf lokalen Netzwerken

Schadsoftware

- Regelmäßiger Virenschutz auf allen Clients
- Regelmäßiger Virenschutz auf allen Servern
- Permanenter Virenschutz auf externen Mailservern, Exchangeservern und Servern bei Zugriff
- Unterschiedliche Virenschutzsoftware
- Personal Firewall
- Regelungen und Schulungen zum Verhalten bei möglichen Angriffsszenarien
- Regelungen zum Download von Software / Blacklist

Übertragungskontrolle, § 64 Abs. 3 Nr. 6 BDSG-NEU

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können

- Protokollierung der FTPS Übertragung auf Ubuntu-Server

Eingabekontrolle, § 64 Abs. 3 Nr. 7 BDSG-NEU

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind, z.B.: Protokollierung, Dokumentenmanagement;

- Protokollierung in der jeweiligen Anwendung je nach Weisung des Auftraggebers

Transportkontrolle, § 64 Abs. 3 Nr. 8 BDSG-NEU (Weitergabekontrolle)

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Geregelter und überwachter Transport von Datensicherungsbändern
- Nutzung kryptographischer Verfahren bei WLAN, eMail-Kommunikation, Blackberry etc.
- Regelungen und Prozessvorgaben zur Nutzung, Vergabe und Sicherheit von Remote Access Nach Weisung des Auftraggebers
- Datenschutzkonformes Löschen und Entsorgen von Festplatten

Datenintegrität, § 64 Abs. 3 Nr. 11 BDSG-NEU

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

- Regelungen für den Fall von übergeordneten oder anwendungsbezogenen Notfällen (Bestandteil Betriebshandbuch)
- Brandschutzkonzept
- Notfallhandbuch
- Aushänge / Handzettel / Verhaltensregelungen für Notfälle
- Shutdown-Liste Server
- Regelmäßige Notfallübungen
- Überwachung des Rechenzentrums und automatisierte Benachrichtigung bei Ausfall oder Störung

Trennbarkeit, § 64 Abs. 3 Nr. 14 BDSG-NEU

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können, z.B. Mandantenfähigkeit, Sandboxing;

- Physikalische und logische Trennung von Anwendungen
- Physikalische und logische Trennung bei der Datenhaltung
- Mandantenfähigkeit bei Anwendungen je nach Vorgabe Auftraggeber
- Trennung von Test-, Entwicklungs- und Produktivsystemen ja nach vertraglichen Regelungen mit dem Auftraggeber

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Pseudonymisierung ist auf Grund des Geschäftsmodells nur durch den Auftraggeber möglich.

Die Produktivverarbeitung erfolgt auf Grund des Dienstleistungsvertrages mit den zur Verfügung gestellten Daten

2. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Rasche Wiederherstellbarkeit, Art. 32 Abs. 1 lit. c DS-GVO, , § 64 Abs. 3 Nr. 9 BDSG-NEU

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können

Datensicherungen

- Regelmäßiges Backup aller Server und Datenbanken abhängig vom Kundenauftrag
- Prozess zur Aufnahme in die Sicherung von neuen Systemen

Systeme

- Redundanter Internetzugang
- Redundante Firewalltechnologie
- Alle Systeme des Mailsystems sind redundant ausgelegt
- Anwendungsspezifische Redundanz bei Systemen und Datenbanken je nach Vorgaben des Auftraggebers

Zuverlässigkeit, § 64 Abs. 3 Nr. 10 BDSG-NEU

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

Systeme

- Redundanter Internetzugang
- Redundante Firewalltechnologie
- Alle Systeme des Mailsystems sind redundant ausgelegt
- Anwendungsspezifische Redundanz bei Systemen und Datenbanken je nach Vorgaben des Auftraggebers

Asset-Verwaltung (Wartung / Kapazitätsmanagement)

- Angabe von Wartung / Kapazitäten / Zuständigkeiten etc. je Betriebsmittel
- Abbildung aller virtuellen Systeme

Verfügbarkeitskontrolle, § 64 Abs. 3 Nr. 13 BDSG-NEU

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Notfallmanagement

- Regelungen für den Fall von übergeordneten oder anwendungsbezogenen Notfällen (Bestandteil Betriebshandbuch)
- Brandschutzkonzept
- Notfallhandbuch
- Aushänge / Handzettel / Verhaltensregelungen für Notfälle
- Shutdown-Liste Server
- Regelmäßige Notfallübungen
- Überwachung des Rechenzentrums und automatisierte Benachrichtigung bei Ausfall oder Störung

Monitoring

- Überwachung aller wichtigen Systeme und Anwendungen
- Dokumentation der Verfügbarkeiten
- Fehleranalyse bei Störungen an Systemen oder
- Ermittlung der Verfügbarkeiten durch Monitoring von innen nach außen
- Referenztransaktionen Netzwerkkomponenten

3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management;

Gemäß Datenschutzrichtlinie der CSW Peripheriesysteme GmbH

Incident-Response-Management;

Monitoring

- Überwachung aller wichtigen Systeme und Anwendungen
- Dokumentation der Verfügbarkeiten
- Fehleranalyse bei Störungen an Systemen oder
- Ermittlung der Verfügbarkeiten durch Monitoring von innen nach außen
- Referenztransaktionen Netzwerkkomponenten

DS-Panne

Verfahren gemäß interner Verfahrensanweisung

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

- Datenlieferung der nur erforderlichen Daten durch den Auftraggeber gemäß Dienstleistungsauftrag.
- Isolierte Mandantenspezifische Verarbeitung.
- Prozess zur Vergabe , Entzug und Kontrolle von Berechtigungen (Genehmigung, Freigabe und regelmäßige Überprüfung durch Personalverantwortlichen)

- Vergabe, Überwachung und Dokumentation produktbezogener Berechtigungen durch Produktverantwortlichen

Auftragskontrolle, § 64 Abs. 3 Nr. 12 BDSG-NEU

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Rahmenverträge und Leistungsscheine

- Vertragliche Festlegungen zu Art, Umfang und Verfügbarkeit der Auftragsdatenverarbeitung generell und je Anwendung

Personalsicherheit

- Verpflichtung
- Regelmäßige Unterweisungen und Schulungen