Vertrag über die Verarbeitung von personenbezogenen Daten

im Auftrag des

Social media - Kunden
(im Folgenden: Auftraggeber)

durch die

Sellwerk GmbH & Co. KG

Pretzfelder Straße 7-11, 90425 Nürnberg

(im Folgenden: Auftragnehmer)

Präambel

Der Auftraggeber hat den Auftragnehmer im Rahmen der datenschutzrechtlich bestehenden Sorgfaltspflichten als Dienstleister für die Erstellung und Pflege seiner Webseite ausgewählt. Diese Vereinbarung enthält nach dem Willen der Parteien den Auftrag zur Auftragsverarbeitung in dem vertraglich beschriebenen Umfang und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Auftragsverarbeitung.

1. Gegenstand des Auftrags, Art, Zweck und Umfang der Datenverarbeitung

(1) Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag und nach Weisung des Auftraggebers.

(2) Die vom Auftragnehmer zur Erfüllung der vertraglichen Verpflichtungen zu verwendenden Daten und der Kreis der Betroffenen sind in **Anlage 1** bestimmt.

(3) Die Tätigkeit des Auftragnehmers im Rahmen dieser Vereinbarung bestimmt sich aus der konkreten Tätigkeitsbeschreibung in Anlage 1 sowie ergänzender Einzelweisungen.

2. Verantwortlichkeit des Auftraggebers und Weisungsgebundenheit des Auftragnehmers

(1) Allein der Auftraggeber für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchgeführten Verarbeitung personenbezogener Daten durch den Auftragnehmer im Hinblick auf die jeweils anwendbaren Bestimmungen des Datenschutzrechts verantwortlich.

(2) Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich im Rahmen dieser vertraglichen Vereinbarung und der speziellen Einzelweisungen des Auftraggebers. Der Auftragnehmer ist nicht berechtigt, die Daten des Auftraggebers in einer Weise zu verarbeiten, die diesen Vorgaben widersprechen.

(3) Absatz (2) wird eingeschränkt, soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer Datenverarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (vgl. Art. 28 Abs. 3 a) DSGVO).

3. Weisungen und weisungsberechtigte Personen

(1) Der Auftraggeber oder ein entsprechend Bevollmächtigter werden sämtliche Weisungen in Textform (schriftlich, per Fax oder E-Mail) erteilen. Sofern ausnahmsweise mündliche Weisungen erteilt werden, müssen diese unverzüglich mit Fax oder E-Mail bestätigt werden.

(2) Soweit Weisungen oder Hinweise nach dieser Vereinbarung gegenüber der anderen Partei zu erfolgen haben, sind diese an die in Anlage 2 genannten Personen zu richten.

(3) Jede Partei kann die angegebenen Kontaktpersonen durch Erklärung in Textform gegenüber der anderen Partei ändern. Die Änderung wird unverzüglich nach Zugang der Änderungserklärung wirksam.

4. Pflichten des Auftragnehmers

(1) Eine Berichtigung, eine Löschung von Daten oder eine Einschränkung der Verarbeitung ist dem Auftragnehmer nicht gestattet, es sei denn, es liegt eine entsprechende Weisung vor oder die Löschung erfolgt nach Ziffer 14 dieses Vertrages (Vertragsbeendigung). Anträge von Betroffenen auf Berichtigung, Löschung oder Sperrung sind unverzüglich an den Auftraggeber weiterzuleiten.

(2) Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers. Falls eine Ausnahme vom Auftraggeber genehmigt wurde, muss ein angemessenes Schutzniveau sichergestellt werden, das die Vorgaben der Art. 44 ff. DSGVO erfüllt.

5. Vertraulichkeit der Datenverarbeitung und Weisungsgebundenheit von Mitarbeitern

(1) Der Auftragnehmer ist verpflichtet sicherzustellen, dass seine Mitarbeiter, die Zugang zu personenbezogenen Daten im Rahmen der Auftragserfüllung haben, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten. Dies gilt nicht, wenn der Dienstleister nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung der vertragsgegenständlichen personenbezogenen Daten verpflichtet ist.

(2) Der Auftragnehmer ist verpflichtet, alle Mitarbeiter, die zur Verarbeitung der im Rahmen dieses Vertrages weitergegebenen Daten befugt sind, zur Vertraulichkeit zu verpflichten. Sie sind einer angemessenen vertraglichen Verschwiegenheitspflicht zu unterwerfen.

6. Datenschutzbeauftragter

(1) Der Auftragnehmer hat – sofern er hierzu gesetzlich verpflichtet ist – einen qualifizierten Beauftragten für den Datenschutz bestellt, dessen Name und Kontaktdaten auf Anfrage mitgeteilt werden.

7. Bearbeitung von Anfragen – Betroffenenrechte

(1) Der Auftragnehmer soll den Auftraggeber per E-Mail unverzüglich ab Kenntnisnahme von jedwedem Empfang von Anfragen oder Aufforderungen, die von einer Datenschutzaufsichtsbehörde oder einem Journalisten bezüglich des Gegenstandes dieses Vertrages gemacht wird, informieren.

(2) Der Auftraggeber ist als Verantwortlicher auch für die Wahrung der Betroffenenrechte zuständig. Betroffenenrechte sind ausschließlich gegenüber dem Auftraggeber wahrzunehmen. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten, insbesondere auf Auskunft, Berichtigung, Einschränkung, Datenübertragbarkeit oder Löschung erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

(3) Der Auftragnehmer wird den Auftraggeber über entsprechende Anfragen von Betroffenen unverzüglich informieren.

8. Sub-Dienstleister

(1) Die Einbeziehung von weiteren Unternehmen in die vertragsgegenständliche Datenverarbeitung (=Sub-Dienstleistern) ist nur mit Zustimmung des Auftraggebers zulässig. Der Auftragnehmer wird dem Auftraggeber die Einbeziehung weiterer Sub-Dienstleister und die Überlassung von personenbezogenen Daten des Auftraggebers an diese zur Verarbeitung vorab in Textform ankündigen. Widerspricht der Auftraggeber diesem Einsatz nicht innerhalb von 4 Wochen nach der Anzeige, gilt die Zustimmung des Auftraggebers als erteilt.

(2) Voraussetzung für eine Zustimmung zur Einschaltung weiterer Sub-Dienstleistern ist dessen konkrete Benennung mit Namen und Kontaktdaten zusammen mit weiteren Informationen über den konkreten Bereich und den Umfang der vorgesehenen Datenverarbeitung. Weiterhin wird der Auftragnehmer die datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter übertragen.

(3) Der Auftraggeber wird eine Zustimmung zur Beauftragung von Sub-Dienstleistern nicht unbillig verweigern. Sofern der Auftraggeber der Einbeziehung eines weiteren Dienstleisters widerspricht, kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtigte Änderung nicht zumutbar ist – den Vertrag gegenüber dem Auftraggeber innerhalb von vier Wochen nach Zugang des Widerspruchs des Betroffenen kündigen.

(4) Die vorab genehmigten Sub-Dienstleister sind in **Anlage 3** angeführt.

(5) Nicht als genehmigungspflichtiges Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9. Festlegung der technischen und organisatorischen Maßnahmen

(1) Die Auswahl des Auftragnehmers erfolgt insbesondere aufgrund der Einschätzung, dass er hinreichende Garantien dafür bietet, die technischen und organisatorischen Maßnahmen zur Datensicherheit einzuhalten und die Verarbeitung der personenbezogenen Daten im Einklang mit Anforderungen der gesetzlichen Regelungen vorzunehmen und den Schutz der Rechte der Betroffenen zu gewährleisten.

(2) Der Auftragnehmer stellt die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der zur Datenverarbeitung eingesetzten Systeme und Dienste sicher. Zudem wird er sicherstellen, dass die Verfügbarkeit der Daten und der Zugang zu ihnen bei einem physischen oder techni-

schen Zwischenfall rasch wiederhergestellt wird und dass eine möglichst weitgehende Transport- und Speicherungsverschlüsselung eingesetzt wird. Der Auftragnehmer gewährleistet für seinen Verantwortungsbereich die Umsetzung der angemessenen technischen und organisatorischen Maßnahmen entsprechend den in **Anlage 4** getroffenen Regelungen, um die Einhaltung der Datenschutzvorschriften zu gewährleisten.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen bedürfen der Zustimmung des Auftraggebers.

10. Allgemeine Kontroll- und Hinweispflichten des Auftragnehmers

(1) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Vorschriften über den Datenschutz verstößt, weist der Auftragnehmer den Auftraggeber unverzüglich in Textform darauf hin. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird. Eine materiell-rechtliche Prüfung steht dem Auftragnehmer nicht zu.

(2) Ist der Auftragnehmer der Ansicht, dass die vom Auftraggeber getroffenen Anordnungen zur Datensicherheit unzureichend sind, informiert er unverzüglich den Auftraggeber.

11. Mitzuteilende Verstöße des Auftragnehmers / Datenverlust

(1) Der Auftragnehmer unterstützt unter Berücksichtigung der Art der Datenverarbeitung und den zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO.
.

12. Kontrolle durch den Auftraggeber

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO genannten Pflichten zur Verfügung und ermöglicht entsprechende Überprüfungen.

(2) Das Recht zur Auditierung der Datenverarbeitung hat das Ziel, die Einhaltung der dem Auftragsverarbeiter obliegenden Pflichten hinsichtlich der vertragsgegenständlichen Datenverarbeitung und der Einhaltung der DSGVO zu überprüfen. Dieser Nachweis soll primär durch Vorlage unabhängiger Prüfberichte (etwa durch den Datenschutzbeauftragten) bzw. Zertifizierungen erfolgen. Sofern der Auftraggeber auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel hinsichtlich der vorgelegten Prüfberichte bzw. Zertifizierungen geltend macht, kann er Vor-Ort-Kontrollen durchführen. Gleiches gilt für die Fälle, in denen es zu meldepflichtigen Vorfällen nach Art. 33 DSGVO gekommen ist. Sofern solche Vor-Ort-Kontrollen erfolgen, sind diese als Stichprobenkontrolle in den für die Durchführung der Auftragsverarbeitung relevanten Bereichen auszugestalten und rechtzeitig im Voraus – in der Regel 14 Kalendertage – in Textform anzuzeigen. Das gleiche gilt für anlasslose Vor-Ort-Kontrollen.

(3) Die Durchführung von Vor-Ort-Kontrollen darf den Geschäftsbetrieb nicht über Gebühr stören oder missbräuchlich sein. Der Auftragnehmer ist berechtigt, für die Durchführung von Vor-Ort-Kontrollen ein angemessenes Entgelt zu verlangen.

(4) Gemäß den anwendbaren Datenschutzvorschriften unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen

des Auftraggebers wird der Auftragnehmer den Auftraggeber im Rahmen von Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten Gegenstand des Aufsichtsverfahrens ist.

13. Vertragsdauer und Kündigungsrecht

(1) Für diese Vereinbarung werden folgende Regelungen zu Vertragsdauer und Kündigungsrecht getroffen: diese Vereinbarung wird auf unbegrenzte Zeit geschlossen und kann mit einer Frist von vier Wochen zum Ende eines Quartals gekündigt werden.

(2) Der Auftraggeber kann den dieser Datenverarbeitung zugrundeliegenden Vertrag jederzeit ohne Einhaltung von Kündigungsfristen kündigen, wenn

- ein schwerwiegender Verstoß vom Auftragnehmer gegen datenschutzrechtliche Bestimmungen oder Festlegungen dieses Vertrages vorliegt, oder
- wenn der Auftragnehmer den Zutritt des Auftraggebers oder eines entsprechend Beauftragten zu den Betriebsräumen, in denen Daten auf Grund dieses Vertrages verarbeitet werden, vertragswidrig verweigert.

14. Erledigung von Aufträgen/Beendigung des Vertragsverhältnisses

(1) Sofern keine anderweitige Weisung erteilt wird, gelten folgende Regelungen:

(a) Im Fall der Durchführung von Einzelaufträgen hat der Auftragnehmer die von dem Auftraggeber zur Verfügung gestellten personenbezogenen Daten drei (3) Monate nach Durchführung des Einzelauftrages unwiderruflich zu löschen.

(b) Sofern die Dauer dieser Vereinbarung der Dauer der Leistungsvereinbarung entspricht und kein Fall eines Einzelauftrages vorliegt, werden die im Rahmen der Vertragsdurchführung angefallenen Daten nur nach gesonderter Weisung des Auftraggebers gelöscht.

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

(3) Sofern sich die Laufzeit dieser Vereinbarung nach der Laufzeit des Hauptvertrages richtet und der Hauptvertrag beendet wird, ist der Auftragnehmer ausschließlich im Rahmen der ordnungsgemäßen Abwicklung des Vertrages auch zu einer weiteren Speicherung und Verarbeitung von Daten über das Ende des Hauptvertrages hinaus berechtigt.

(4) Von den Löschpflichten sind die Daten ausgenommen, die der Auftragnehmer gegenüber den Finanzbehörden zum Nachweis von buchungsrelevanten Vorfällen vorhalten muss. Diese Daten dürfen ausschließlich aus steuerrechtlichen Gründen – sofern nach § 146 AO erforderlich – weiter gespeichert werden. Gleiches gilt für die Daten, die handelsrechtlichen Aufbewahrungspflichten (vgl. § 238 HGB) - unter Berücksichtigung der Vorgaben der GoBD - unterliegen.

Ort, Datum	Unterschrift

15. Anlagen - folgende Anlagen sind Bestandteil des Vertrages:

Anlage 1: Beschreibung der Tätigkeit des Auftragnehmers, incl. Art, Umfang und Zweck der Datenverarbeitung, sowie Beschreibung der Art der Daten und der Betroffenen
Anlage 2: Kontaktpersonen
Anlage 3: Vorab genehmigte Sub-Dienstleister
Anlage 4: Vorgaben zur Datensicherheit

Anlage 1 Art, Umfang und Zweck der Datenverarbeitung, inklusive Beschreibung der Art der Daten und der Betroffenen

Art der personenbezogenen Daten

x Adressdaten	x Kontaktdaten	x Vertragsdaten
☐ Bankverbindungsdaten	x Abrechnungsdaten	☐ Daten zu Mitarbeiterqualifikationen
☐ Videoaufzeichnungen	☐ Kundenhistorie	☐ Planungs- und Steuerungsdaten
☐ besonders schutzwürdig Daten (z.B. zu Gesundheit)	☐ Tonaufzeichnungen	x Online-Nutzungsdaten

Kategorien der Betroffenen

☐ Mitarbeiter	☐ Pensionäre	☐ Auszubildende, Praktikanten, Werkstudenten
☐ Bewerber	☐ Privatkunden	x Firmenkunden
☐ ehemalige Kunden	☐ Interessenten	x Ansprechpartner, Kontaktpersonen
☐ Lieferanten	☐ Handelsvertreter	☐

Verwendungszweck der Daten/Tätigkeitsbeschreibung

x Vertragsdurchführung von: Suchmaschinenoptimierung von Webseiten

Der Auftraggeber erteilt dem Auftragnehmer die Weisung, die hier angeführten Daten der Betroffenen für den genannten Zweck zu verwenden. Änderungen können jederzeit als gesonderte Weisung erfolgen.

Anlage 2
Weisungsberechtigte Personen, Datenschutzbeauftragter

1. Weisungsberechtigte des Auftraggebers:

Ansprechpartner auf Seiten des Auftraggebers ist der Geschäftsführer oder eine von ihm bevollmächtigte Person.

2. Weisungsempfänger des Auftragnehmers

Ansprechpartner auf Seiten des Auftragnehmers:

Funktion
derzeit besetzt mit:
Name: Daniel Leitenbacher
E-Mail: daniel.leitenbacher@sellwerk.de
Telefon: +49 911 3409 571

Anlage 3
Genehmigte Sub-Dienstleister

Folgende Sub-Dienstleister dürfen vom Auftragnehmer eingesetzt werden:

FIRMA	Anschrift/ Sitz	Aufgabenbereich
Meta Platforms Inc.	1 Meta Way, Menlo Park, CA 94025, USA	Werbeanzeigenmanager
Matchcraft LLC	2701 Ocean Park Blvd, Suite 220, Santa Monica, California 90405, USA	Zusammenfassung der Kampagnendaten und Reporting an den Kunden
etracker GmbH	Erste Brunnenstr. 1, 20459 Hamburg	Tracking auf der Landingpage
excelsea GmbH & Co. KG	Pretzfelder Str. 7-11, 90425 Nürnberg	Generierung einer Call-Tracking-Nummer, danach Reporting an den Kunden
Mono Solutions ApS	Hejrevej 28, 2400 Copenhagen NV, Dänemark	Bei Landingpage: Verwaltung der Website
Website Check GmbH	Beethovenstraße 24, 66111 Saarbrücken	Bei Landingpage: Erstellung von Impressum, Datenschutzerklärung und Cookie-Banner

Anlage 4
Vorgaben zur Datensicherheit

Der Dienstleister ist verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau für die im Rahmen der Auftragsdurchführung verwendeten Daten zu treffen. Diese Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Datenverarbeitung zu treffen. Diese Maßnahmen sollen Vertraulichkeit, Integrität, Verfügbarkeit der Daten bei Vertragsdurchführung sicherstellen.

I. Organisatorische Vorgaben zur Gewährleistung der Datensicherheit

Der Dienstleister unterhält ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung.

II. Technische Maßnahmen zur Gewährleistung der Datensicherheit

Der Auftragnehmer trifft zur Gewährleistung der Datensicherheit folgende Maßnahmen, deren Einhaltung durch entsprechende Kontrollen im Rahmen der organisatorischen Maßnahmen gewährleistet wird:

Schutzziel: Vertraulichkeit

Es ist sicherzustellen, dass keine Person – sowohl Mitarbeiter als auch Dritte - personenbezogene Daten unbefugt zur Kenntnis nimmt.

1 Zutrittskontrolle:

Kontrolle des räumlichen Zutritts zu Datenverarbeitungsanlagen (DV-Anlage) durch Unbefugte. Durch die Zutrittskontrolle soll verhindert werden, dass Personen, die dazu nicht befugt sind, in die Nähe einer DV-Anlage gelangen können. Zur DV-Anlage gehören neben der Zentraleinheit einschließlich der integrierten Laufwerke auch die angeschlossenen Peripherieeinheiten wie Terminals, PCs, Drucker, Plotter und Bandeinheiten usw.

Eine Zutrittskontrolle zu PCs innerhalb von Büroräumen wird z.B. dadurch sichergestellt, dass Maßnahmen ergriffen werden, die verhindern, dass Kunden in die Nähe von PCs gelangen bzw. den Bildschirm einsehen können.

Forderungen
Zutrittsregelung für betriebsfremde Personen; die Umsetzung erfolgt beispielsweise durch folgende Punkte:
• Protokollierung der Zu- und Abgänge von betriebsfremden Personen
• Zentraler Empfangsbereich (Pförtner/Empfang) vorhanden
• Ausgabe von Besucherausweisen
• Aufenthalt von Fremden im gesamten Unternehmensgebäude nur in Anwesenheit von Mitarbeitern
• Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung

Zutrittsregelung für betriebsangehörige Personen; die Umsetzung erfolgt beispielsweise durch folgende Punkte:
• Protokollierung der Zu- und Abgänge von Mitarbeitern
• Code-Nummerntaster mit regelmäßigen Wechsel des Codes

• Chipkarte mit Protokollierung
Festlegung der zutrittsberechtigten Personen für Rechner-/Serverraum
Maßnahmen, damit nur Befugte Zutritt zum Rechner- /Serverraum erhalten
Bereitstellung verschließbarer Schränke/Rollcontainer für Mitarbeiter
Schlüsselregelung, sofern Schlüssel verwendet werden, (verschlossene Türen; Schlüsselausgabe nur an Befugte; Aufbewahrung und Verwendung eines Generalschlüssels)
Maßnahmen der Objektsicherung (z.B. Absicherung von Schächten und Fenstern; Geländeüberwachung)

2 Zugangskontrolle:

Die Benutzung von DV-Anlagen durch unbefugte Personen (nicht befugte Mitarbeiter oder Externe) soll verhindert werden. Bei der Zugangskontrolle geht es um die Frage der Identifikation und anschließender Authentifikation. Die Zugangskontrolle umfasst auch das Ziel, dass kein externer Zugang (z.B. aus dem Internet) auf DV-Anlagen erfolgen kann (Hackerschutz).

Forderungen
Authentisierung der Benutzer gegenüber dem Datenverarbeitungssystem. d.h. Identifikation durch Benutzernamen und Kennwort oder 2-Faktor-Verfahren
Regelungen zur Passwortvergabe • Persönliches Passwort • Mindestens 10 Zeichen, darunter auch Groß- und Kleinbuchstaben und Zahlen; unter 12 Zeichen auch Sonderzeichen; • Vergabe durch Nutzer selbst • Verfall nach vorgegebener Zeit (spätestens nach 6 Monaten) • Zugangssperre nach fünf Fehlversuchen • Keine Weitergabe an Dritte • Vertretungsregelung für Fall der Abwesenheit (Urlaub, Krankheit etc.) • Sperre der zuletzt verwendeten 5 Passworte
Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern
Separate Benutzerkennungen für administrative Zwecke
Regelmäßige Kontrolle der Gültigkeit von Berechtigungen (jährlich)
Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System (Passwortschutz für Bildschirmschoner nach 5 Min. bis 15 Min, je nach Risiko des Missbrauchs)
Automatisierte temporäre Sperrung von Benutzerkonten bei mehrfachen fehlerhaften Anmeldeversuchen.
Abschottung interner Netze gegen Zugriffe von außen (Firewall, Verschlüsselung VPN)
Abschottung von Serversystemen mittels Firewalls

3 Zugriffskontrolle:

Ziel der Zugriffskontrolle ist es, dass Mitarbeiter und befugte Dritte nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können. Darüber hinaus soll sichergestellt werden, dass beim Umgang mit personenbezogenen Daten diese nicht unbefugt gelesen, kopiert, verändert oder entfernt (gelöscht) werden können. Dies gilt sowohl für Daten, die in DV-Systemen gespeichert sind, als auch für solche, die sich auf maschinell lesbaren Datenträgern oder auf

Papier befinden.

Forderungen
Erstellung eines Benutzerprofils d.h. Festlegung von Zugriffsberechtigungen hinsichtlich personenbezogener Daten von Nutzern
Differenzierte Berechtigungen für Lesen, Verändern oder Löschen von Daten
Vergabe von Berechtigungen an Mitarbeiter und Erfüllungsgehilfen nach dem Minimalprinzip; Zugriff auf Anwendungen und Systemkomponenten wird nur gestattet, wenn dieser Zugriff für die konkrete Tätigkeit erforderlich ist.
Erstellung eines Berechtigungskonzeptes • Einrichtung von Administrationsrechten • Verwaltung der Zugriffsrechte durch Systemadministrator
Trennung von Test- und Produktionsbetrieb
Konfiguration der eingesetzten EDV-Geräte dahingehend, dass alle Dienste und Komponenten deaktiviert werden, welche nicht zur Erfüllung seiner Dienstleistungen benötigt werden. Jährliche Überprüfung der ordnungsgemäßen Konfiguration
Vergabe von Berechtigungen muss nachvollziehbar dokumentiert werden und einen Genehmigungsschritt umfassen.
datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger nach dem jeweiligen Stand der Technik unter Beachtung der jeweils gültigen Normen (DIN 66399:2012) oder Beauftragung eines auf Entsorgung von Datenträgern spezialisierten Dienstleisters mit der Entsorgung, der die Datenträger mit derselben oder einer höheren Sicherheitsstufe vernichten wird. Die zur Entsorgung vorgesehenen Datenträger sind während der Lagerung und des Transports mit geeigneten Maßnahmen vor unbefugtem Zugriff zu schützen.
datenschutzgerechte Entsorgung von Makulatur (beispielsweise Fehldrucke von Arbeitslisten, Anschreiben etc.) mittels eines Aktenvernichters der eine nach DIN 66399:2012 definierten Sicherheitsstufe P-4 aufweist, oder Beauftragung eines auf Aktenvernichtung spezialisierten Dienstleister mit der Entsorgung, der die Dokumente mit derselben oder einer höheren Sicherheitsstufe vernichten wird.
schriftliche Regelung zur Zulässigkeit/zum Verbot des Kopierens von Daten
Implementierung von Maßnahmen zum Schutz vor unerlaubten Datenabflüssen (Einschränkungen der USB-Schnittstellen, Data-Leakage-Detection/Prevention/Protection Software, etc.)

4 Trennungskontrolle:

Nach dem Trennungsgebot sind Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt zu verarbeiten (auch: Gebot der Nichtverkettbarkeit). Dadurch soll gewährleistet werden, dass die Zweckbindung personenbezogener Daten durch organisatorische und technische Maßnahmen umgesetzt wird. Besondere Bedeutung hat das Trennungsgebot im Rahmen der Auftragsverarbeitung, wenn z.B. Daten mehrerer Auftraggeber auf einem System gespeichert sind. Sofern das Trennungsgebot nicht durch technische Maßnahmen, wie z.B. eine Zugriffs-Kontroll-Software, erreicht werden kann, ist eine getrennte Speicherung notwendig.

Forderungen
Berechtigungskonzept mit Festlegung der Zugriffsrechte
Mandantenfähige Datenbank

Schutzziel: Integrität

Es ist sicherzustellen, dass informationstechnische Prozesse und Systeme die festgelegten Spezifikationen kontinuierlich einhalten, so dass die mit ihnen zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben.

5 Weitergabekontrolle:

Umfasst sind alle Varianten der Weitergabe von personenbezogenen Daten mittels Datenträgern oder Kommunikationsnetz. Die Weitergabekontrolle soll verhindern, dass Daten bei deren Weitergabe unbefugt verwendet (gelesen, kopiert, verändert oder entfernt/gelöscht) werden können. Der Begriff der Weitergabe umfasst sowohl die Übermittlung an Dritte als auch die Weitergabe im Rahmen der Auftragsverarbeitung zwischen Auftraggeber und Auftragnehmer und an den Betroffenen.

Forderungen
Dokumentation von Datenempfänger, der Transport- /Übermittlungswege, der zur Übermittlung von Daten befugten Personen und der zu übermittelnden Daten
Authentisierte und hinreichend verschlüsselte Übertragung von Daten vor der Weitergabe bei nicht gesicherten Übertragungswegen

6 Eingabekontrolle:

Durch die Eingabekontrolle soll dokumentiert werden, wer für eine (un)zulässige oder fehlerhafte Dateneingabe verantwortlich ist. Ziel ist die Revisionsfähigkeit der Eingabe von personenbezogenen Daten in das DV-System, zu welchem auch nicht vernetzte Einzelarbeitsplätze wie z.B. PCs gehören. Die zu kontrollierende Dateneingabe umfasst sowohl das erstmalige Speichern als auch die Veränderung und Löschung (Entfernung) von Daten.

Forderungen
Führung von nachweisbar erteilten Zugriffsberechtigungen
Protokollierung von Eingabe, Veränderungen oder Löschung personenbezogener Daten
Regelung zu Zugriffsbefugnissen auf erstellte Protokolldaten
Löschungsregelung für Protokolldaten

Schutzziel: Verfügbarkeit

7 Verfügbarkeitskontrolle:

Die vertragsgegenständlichen Daten müssen im Zugriff der Vertragspartner liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können. Die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall muss rasch wiederherzustellen sein. Dazu sind der Schutz der Daten gegen zufällige Zerstörung oder Verlust zu gewährleisten. Mögliche Gefahren sind z.B. Wasserschäden, Blitzschlag, Stromausfall, Brand, Sabotage oder Diebstahl.

Forderungen
formalisiertes Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Alt-Verfahren
unterbrechungsfreie Stromversorgung (USV)
automatische Feuer- und Rauchmeldeanlagen
CO2 Feuerlöschgerät im/vor Serverraum
Sicherung der Datenbestände • Erstellung eines Bestandssicherungskonzeptes • Aufbewahrung der Sicherungskopien an einem sicheren Ort (Auslagerung) • Erstellung von Sicherungskopien nach dem Generationenprinzip in geeigneten zeitlichen Abständen
Rekonstruktion von Datenbeständen • Testläufe bei der Rekonstruktion von Datenbeständen

Redundanz von Hard- und Software sowie Infrastruktur
Vertretungsregelungen für Mitarbeiter

Schutzziel: Belastbarkeit

8 Auftragskontrolle:

Gewährleistung der weisungsgemäßen Auftragsverarbeitung. Der Auftragnehmer hat die ihm erteilten Weisungen einzuhalten, während der Auftraggeber Sorge dafür zu tragen hat, dass seine Weisungen klar und eindeutig sind und befolgt werden.

Forderungen
Kontrolle der Einhaltung von Datensicherheitsbestimmungen durch Auftragnehmer und Meldung, wenn Verstöße vorliegen oder der Verdacht besteht, dass die Datensicherheitsvorgaben unzureichend sind.
Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung der datenschutzrelevanten Vorgaben
Erteilung von Weisungen an die Mitarbeiter hinsichtlich der vorgesehenen Verwendung der Daten als auch des Umfangs der Daten, die für die Auftragsdurchführung erforderlich sind und verwendet werden sollen.

9 Verfahren zur regelmäßigen Überprüfung

Ständige Gewährleistung der Einhaltung der Vorgaben an Datenschutz und IT-Sicherheit. Der Auftragnehmer hat regelmäßig zu überprüfen und dokumentieren, dass die vertraglich geschuldeten Vorgaben eingehalten werden.

Forderungen
Einführung eines Systems zur Rechenschaftspflicht und IT-Governance
Incident-Response Management
Gewährleistung datenschutzfreundlicher Voreinstellungen bei Gestaltung und Betrieb der Datenverarbeitungsprozesse, z. B. durch: • informationelle Gewaltentrennung innerhalb und zwischen verantwortlichen Stellen • Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten • Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme gegenüber im Dialog gesteuerten Prozessen begrenzen • Implementierung automatischer Sperr- und Löschroutinen • Pseudonymisierungs- und Anonymisierungsverfahren • Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren
weitreichende Pseudonymisierung und Verschlüsselung personenbezogener Daten
Meldung von Sicherheitsvorfällen, die im laufenden Betrieb sichergestellt werden
Kontrolle der Wirksamkeit der durchgeführten Maßnahmen mindestens einmal pro Jahr
sichere und ausreichende Default-Einstellung für die Server, durch die ein abgesicherter Wiederanlauf des Serversystems in der vorgesehenen Zeit durchgeführt werden kann.