Vereinbarung Datenspeicherung und -Verarbeitung, Datenschutz:

Autohaus Rainer Kärgel
Kfz-Reparaturen und Handel
Queichtalstr. 51-53
76855 Annweiler-Queichhambach

Webenheimstr. 4
66482 Zweibrücken

Kaiserstr. 97
67661 Kaiserslautern-Einsiedlerhof

Das Autohaus Rainer Kärgel verarbeitet personenbezogene Daten im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO.

Standarddatenschutzklauseln, genehmigte Verhaltensregeln

Das Autohaus Rainer Kärgel speichert keine personenbezogenen Daten außer zur Vertrags-/ Auftragsabwicklung mit dem Kunden. Dazu speichert das Autohaus Rainer Kärgel: Name, Anschrift und Telefonnummer, gegebenenfalls auch die E-Mailadresse und eine Kopie des Kfz-Scheins des zugehörigen Kraftfahrzeugs sowie der Identifikation des Auftraggebers. Das Autohaus Kärgel betreibt keine weitergehende Datenverarbeitung oder Datenänderungen. Alle Personen welche Einsicht in personenbezogene Daten haben sind zur Verschwiegenheit verpflichtet. Personenbezogene Daten werden in besonders geschützten Umgebungen mit geschütztem Zugang und beschränktem Zugriff gespeichert.

Das Autohaus Rainer Kärgel erklärt sich damit einverstanden, dass Auftraggeber — grundsätzlich nach Terminvereinbarung — berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Das Autohaus Rainer Kärgel sichert zu, dass es, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen wird das Autohaus Rainer Kärgel nur nach vorheriger Weisung oder schriftlicher Zustimmung durch den Auftraggeber erteilen. Das Autohaus Kärgel gibt keinerlei Daten an Dritte weiter außer:

- bei Anfragen offizieller deutscher Ermittlungsbehörden.

- Die notwendigen Daten für die Hauptuntersuchung an den TÜV Rheinland-Pfalz. Der TÜV Rheinland-Pfalz erinnert unsere Kunden an die fällige HU/AU mit einem Erinnerungsschreiben.

- Für die Teilebestellung geben wir die Fahrzeugdaten an die Teilehersteller weiter.

- Personenbezogen Daten werden in der Software KfzWIN gespeichert. Hierbei gilt zusätzlich die Datenschutzvereinbarung von TopMotive und der DVSE GmbH unter www.msdas.de.

- Abrechnungsdaten werden an den Steuerberater Rieter und Schehl, Bahnhofstr. 21 in 76855 Annweiler weitergegeben. Die Abrechnungsdaten werden in der Datev Software verarbeitet. Hierzu gilt die gesonderte Datenschutzvereinbarung der Datev AG, Paumgarnterstr.6-14, 90329 Nürnberg, www.datev.de.

- Die Umsatzsteuererklärung wird mit der Elster Software erledigt. Hier gilt die gesonderte Datenschutzverordnung der Deutschen Finanzverwaltung.

- Im Auftrag erfolgen eventuelle weitere Datenweitergaben, im Einvernehmen mit dem Kunden, an Kfz-

Gutachter, die Stadtverwaltung, Versicherungen oder Rechtsanwälte.

Das Autohaus Rainer Kärgel bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

Das Autohaus Rainer Kärgel verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages/Auftrages fort.
Das Autohaus Rainer Kärgel sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Das Autohaus Rainer Kärgel überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinen Betrieben.
Beim Autohaus Rainer Kärgel ist als Beauftragte(r) für den Datenschutz Weis Consulting e.K. Geschäftsführer Dipl.-Inform. Karl-Heinz Weis - Zweibrücker Str. 35a - 66953 Pirmasens, bestellt. Ein Wechsel des Datenschutzbeauftragten ist unverzüglich mitzuteilen.

Weisungen der Auftraggeber sind für ihre Geltungsdauer und anschließend noch für drei (3) volle Kalenderjahre aufzubewahren. Ergibt sich nach Überlassung der personenbezogenen Daten an den Auftragnehmer, dass ein Havarist keine vertraglichen Ansprüche gegen den ADAC hat (sogenannte „Selbstzahler-Vermittlungen“), so wird das Autohaus Rainer Kärgel ab dem Zeitpunkt der Klärung und Mitteilung selber Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO und beachtet die Vorgaben nach BDSG und DS-GVO.

Die Verpflichtung gemäß § 5 BDSG aller Mitarbeiter, die auf personenbezogene Daten der Auftraggeber zugreifen können, werden vor Auftragsbeginn durchgeführt. Wo zutreffend, sind die beteiligten Mitarbeiter auch auf das Fernmeldegeheimnis verpflichtet. Die Mitarbeiter sind auf den § 17 UWG verpflichtet. Zur Auftragsvergabe werden die beteiligten Mitarbeiter über die sich aus dem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung nachvollziehbar belehrt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen. Die Nutzung mobiler Endgeräte (Smartphones und Tablets, Laptops) mit der PORTA II App durch Mitarbeiter des Auftragnehmers bleibt davon unberührt.

Zutrittskontrolle: Der unbefugte räumliche Zutritt wird verhindert. Das Betriebsgelände liegt in einem Gewerbegebiet. Das Betriebsgelände ist eingezäunt. Die Besucher müssen sich anmelden und werden begleitet. Die Gebäudetüren sind einbruchhemmend. Es gibt eine dokumentierte Schlüsselaus- und -rückgabe (Schlüsselbuch). Brandmeldeanlagen, Feuer- und Rauchmelder sind in den Betriebsräumen installiert.

Zugangskontrolle: Das Eindringen Unbefugter in die DV-Systeme wird verhindert.

Benutzeranmeldung: Jeder Anwender hat einen eigenen Benutzernamen und ein eigenes Passwort. Eine automatische Anmeldung ist nicht möglich. Trivialpasswörter werden ausgeschlossen. Es erfolgt eine zwingende Verwendung von Zahlen, Groß- und Kleinbuchstaben und teilweise Sonderzeichen. Die Deaktivierung des Bildschirmschoners ist nur mit Passworteingabe möglich. Das LAN ist mit einer Firewall gegen das Internet abgeschottet. Alle PCs sind mit Firewalls und mit einem Anti-Viren-Programm ausgestattet. Die Anti-Viren-Programme werden automatisch mit den neusten Anti-Viren-Signaturen versehen. Sicherheits- / Programmupdates werden regelmäßig eingespielt. Die WLAN Nutzung unterliegt der Nutzung von WPA/WPA2 Verschlüsselung. Die Passwortvergabe unterliegt den Passwortkonventionen. Fernwartung wird genutzt, die Übertragung erfolgt verschlüsselt, die Fernwartung wird protokolliert. Die Administration der IT Systeme erfolgt extern durch Weis Consulting e.K., Zweibrücker Str. 35a, 66953 Pirmasens, www.weis-consulting.de. Verträge/AGBs gem. § 11 BDSG mit externen Dienstleistern liegen vor und können u.a. eingesehen werden u.a. unter http://www.weis-consulting.de/agb.htm.

Datenträger: Schreibender Zugriff auf externe Datenträger ist möglich für System und Datensicherung. Es gibt einen Datenträger pro System. Datenbestände auf externen Datenträgern sind verschlüsselt. Es besteht ein

explizites Verbot zur Nutzung privater Speichermedien. Die Vernichtung von Papierdokumenten erfolgt mittels Schredder / bzw. Dienstleister. Die Vernichtung von Festplatten, CD, DVD etc. erfolgt durch einen zertifizierten Entsorger gem. § 11 BDSG via unserem externen IT-Dienstleister.

Es wird eine **Protokollierung der An- und Abmeldung**, durch die Systemprotokollierung durchgeführt.

Die weisungsgemäße Auftragsdatenverarbeitung gem. § 11 BDSG ist gewährleistet. Für die Auftragsdatenverarbeitung (ADV) gem. § 11 BDSG liegen die dokumentierten Vertragsverhältnisse gem. § 11 BDSG vor und die Vorgaben des § 11 BDSG und die Weisungen sind bekannt, werden eingehalten und kontrolliert.

Die Daten sind gegen zufällige Zerstörung oder Verlust geschützt: Einbruchhemmende Türen, Unterbrechungsfreie Spannungsversorgung, separate Absicherung jedes Stromkreises und durch Spannungsversorgung mit Netzfilter.

Die Daten werden gem. eines Sicherungskonzepts gesichert (noch nicht dokumentiert).

Systempasswortе sind für den Notfall sicher hinterlegt.

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden auch getrennt verarbeitet. Es erfolgt eine Mandantentrennung durch Software und eine logische Trennung der Daten.

Datenschutzmanagement: Die Aufbewahrung der elektronischen Protokolle ist geregelt. Es gibt Regelungen für die Sicherung des Datenbestandes. Ein Konzept zur Meldung von Datenpannen existiert und wird umgesetzt.

Einwilligungserklärung des Kunden

Die Einwilligungserklärung erfolgt freiwillig und kann jederzeit widerrufen werden.
Das Unternehmen nimmt den Schutz der Kundendaten ernst und möchte,
dass sich jeder Kunde beim Besuch unserer Geschäftsräume wohlfühlt.
Der Schutz der individuellen Daten ist für uns ein wichtiges Anliegen, das
wir bei unseren Geschäftsprozessen mit hoher Aufmerksamkeit berücksichtigen.

Unabhängig vom Zustandekommen eines etwaigen Vertrages (Kaufvertrag, Serviceauftrag, Mietvertrag, Kreditauskünfte etc.) und der damit verbundenen gesetzlich erforderlichen Erhebung personenbezogener Daten zur Vertragsabwicklung (gem. § 28 Abs. 1 Satz BDSG) willigt der Auftraggeber ein, gegebene personenbezogener Daten, insbesondere zu Name, Anschrift, Telefon, Fax, Mail, Handy, evtl. Beruf und Hobbys, in Verbindung mit den technischen Daten des Fahrzeug durch das oben genannte Autohaus zu eigenen Zwecken, insbesondere zur Kundenbetreuung und Auftragsbearbeitung erhoben, gespeichert, verarbeitet und genutzt werden können (siehe hierzu nachfolgende Erläuterungen).

Allgemeines:
Unter gesetzlichen Regelungen ist zu verstehen, dass z.B.
Vorhaltefristen gegenüber Behörden wie Kraftfahrtbundesamt,
Polizei usw. zur Speicherung Ihrer persönlichen Daten
führen können, unabhängig von der hier abgegebenen

Einwilligungserklärung. Darüber hinaus speichern wir persönliche
Daten nur soweit ein zulässiges berechtigtes Interesse unsererseits
vorliegt. Dies kann im Einzelfall z.B. eine Ausweiskopie bei Probefahrten,
die Adressspeicherung zur Interessentenpflege oder Ähnliches
sein.

Eigene Zwecke der Datenerhebung, Speicherung, Verarbeitung und Nutzung:

Im Sinne von Kundenbetreuungen
Schriftliche, elektronische und telefonische Kontaktaufnahme

z.B. zur Einladung zu Veranstaltungen, zur Informationen
über technische Neuerungen zu Ihrem Fahrzeug, zur Benachrichtigung
bei TÜV und AU-Fälligkeit

Im Sinne von persönlichen Kundeninformationen:
Kontaktaufnahme z.B. wegen Rückrufaktionen für Ihr Fahrzeug.
Auslauf eines Leasing / Finanzierungvertrages oder Neukaufoption
für Ihr bestehendes Fahrzeug.

Im Sinne von Zufriedenheitsbefragungen:
Nach der Durchführung eines Auftrages in unserem Hause,
kontaktieren wir Sie schriftlich, elektronisch oder telefonisch
bezüglich Ihrer Zufriedenheit der von uns durchgeführten
Arbeiten. Dies kann auch durch ein von uns beauftragtes
Unternehmen geschehen.

Senden Sie eine E-Mail an info@autohaus-kaergel.de mit Ihren Fragen oder Kommentaren.

ADAC Mobilitätspartner

Art der zu verarbeitenden Daten Kreis der Betroffenen Auftragsdauer Weisungsberechtigte des Auftraggebers und Weisungsempfänger im Sinne von § 1 des ADAC Rahmenvertrages sowie gem. Teil A Ziff. 1 des Mobilitätspartner-Vertrages

• Personenstammdaten (Name, Anschrift)
• Kommunikationsdaten wie Telefon, E-Mail
• Vertragsstammdaten (Angaben zur Mitgliedschaft; Angaben zu familiären Verbindungen)
• Zahlungsdaten
• Steuerungsdaten (Angaben zum konkreten Hilfefall, wie Standort, KFZ mit amtlichen Kennzeichen, Zielort für die Hilfeleistung Abschleppen, Pick-up)
• Fotos unfallbeteiligter KFZ mit Kennzeichen (keine Personen)
• Mitglieder
• Kunden
• Beschäftigte
• Dienstleister
• Unfallverursacher
Unbefristet mit Kündigungsfrist gem. § 13 des ADAC Rahmenvertrages
Weisungsberechtigte des Auftraggebers:
• Leitung HMN: Hr. D. Michel
• Leitung PNA: Fr. M. Brenner
• Leitung PNI: Hr. Dr. D. Syring
T 089 76 76 0, E-Mail: amp@adac.de
Weisungsempfänger des Auftragnehmers:
• Autohaus Rainer Kärgel Eigentümer Rainer Kärgel Queichtalstr. 51b 76855 Annweiler Tel.: 06346 96280
Geschäftsführer Dennis Gaede Kaiserstr. 97 67661 Kaiserslautern Einsiedlerhof Tel.: 0631 / 62489766
Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110272 Seite A2-1
Annex 2 Nachweis Technische und organisatorische Maßnahmen (TOM) AMP Nr. 110272
Erläuterung: Die technischen und organisatorischen Maßnahmen (TOM) – und deren Dokumentation – sind das Herzstück des Datenschutzes eines

Unternehmens. Aus Art. 32 DSGVO ergibt sich die Verpflichtung eines Unternehmens, das selbst oder im Auftrag personenbezogene Daten verarbeitet, angemessene technische und organisatorische Maßnahmen umzusetzen und zu dokumentieren. Diese Anlage und vor allem Checkliste zu den technischen-organisatorischen Maßnahmen ist vom Auftragsverarbeiter zwingend entsprechend seiner innerbetrieblichen Organisation auszufüllen. Die innerbetriebliche Organisation ist vom Auftragsverarbeiter so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Bitte kreuzen Sie die Maßnahmen, welche zutreffen an und geben eine kurze Erläuterung dazu ab.

Eingesetzte Unterauftragnehmer bei AMP Nr. 110272

Nr. 1

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

Steuerberater Rieter und Schehl

Verarbeitete Datenkategorien

Abrechnungsdaten

Angaben zur Tätigkeit

Steuerberater

Ort der Datenverarbeitung

Bahnhofstr. 21, 76855 Annweiler

Nr. 2

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

Lawa Solutions

Verarbeitete Datenkategorien

Flotten-Management

Angaben zur Tätigkeit

Automobil-Logistik

Ort der Datenverarbeitung

Zu den Mühlen 19, 35390 Giessen

Nr. 3

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

WM SE

Verarbeitete Datenkategorien

Ersatzteilbestellungen

Angaben zur Tätigkeit

Automobil-Ersatzteil Großhändler

Ort der Datenverarbeitung

Pagenstecherstraße 121 49090 Osnabrück

Nr. 4

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110272 Seite A2-2
TÜV Rheinland-Pfalz

Verarbeitete Datenkategorien

Kfz- und Halterdaten

Angaben zur Tätigkeit

Hauptuntersuchung, Abgasuntersuchung, Durchführung und Benachrichtigung

Ort der Datenverarbeitung

Horstschanze 46, 76829 Landau in der Pfalz

Art der verarbeiteten Daten bei AMP Nr. 110272

☒Berufliche Kontakt- und (Arbeits-)Organisationsdaten
Steuerberater: Bei Mitarbeitern, Name, Vorname, Anschrift, Personalnummern, Anwesenheit, Gehalt, Krankenkasse, Sozialversicherungsnummer, Vermögenswirksame Leistungen, bei Kunden und Lieferanten die Rechnungen / Belege, eigene Bankdaten Kontobewegungen, Kassenbuch

☒Daten zu beruflichen Verhältnissen

Steuerberater: Betriebszugehörigkeit, Aufgaben, Eintritts und Austritt, Tarifgruppe, Entgeltabrechnung, Sonderzahlungen, Pfändung, tägliche Anwesenheitszeiten, Abwesenheitsgründe,

☒Private Kontakt- und Identifikationsdaten

Steuerberater: Name, Vorname, Anschrift, Geburtsdatum/-ort, Identifikationsnummern, Kontoverbindungen

☐Vertragsdaten

☒Positionsdaten

Flottenmanagement: GPS, Bewegungsprofil der Betriebs Kfz, Fahrer, Fahraufträge

☐Daten zu persönlichen Verhältnissen

☒Bonitäts- und Bankdaten

Steuerberater: Kontoverbindung, Kontobewegungen, Kassenbuch

☐Besonders sensible personenbezogene Daten

☒Sonstiges

Ersatzteilbestellungen und TÜV: Fahrzeugdaten teilweise inkl. Halterdaten und Kfz-Schein, Teile-Bestellungen, durchgeführte und durchzuführende Reparaturen.

Betroffene Personengruppen bei AMP Nr. 110272

☒Mitarbeiter des Auftraggebers/des Verantwortlichen

Nur zur Verschwiegenheit Verpflichtete Geschäftsinhaber, Teilhaber und Mitarbeiter

☐Mitarbeiter dritter Unternehmen

☒Kunden/ Mitglieder des Auftraggebers/ Verantwortlichen

Mitarbeitern, Name, Vorname, Anschrift, Ausweisdaten, Führerscheindaten, Daten im Kfz-Schein, Angebote, Auftragsdaten, Rechnungsdaten

☒Sonstige Geschäftspartner

Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110272 Seite A2-3
Die Administration der IT-Systeme erfolgt extern durch Weis Consulting e.K., Zweibrücker Str. 35a, 66953 Pirmasens, www.weisconsulting.de. Verträge/AGBs gem. § 11 BDSG mit externen Dienstleistern liegen vor und können u.a. eingesehen werden u.a. unter http://www.weis-consulting.de/agb.htm. Die internen Abrechnungsdaten werden in der Datev Software verarbeitet. Hierzu gilt die gesonderte Datenschutzvereinbarung der Datev AG, Paumgarnterstr.6-14, 90329 Nürnberg, www.datev.de. Die Umsatzsteuererklärung wird mit Elster erledigt. Hier gilt die gesonderte Datenschutzverordnung der Deutschen Finanzverwaltung. Im Auftrag erfolgen eventuelle weitere Datenweitergaben, im Einvernehmen mit dem Kunden, an Kfz-Gutachter, die Stadtverwaltung, Versicherungen oder Rechtsanwälte. Die externe Rechnungsschreibung erfolgt durch KfzWin Software der DVSE Gesellschaft für Datenverarbeitung, Service und Entwicklung mbH Lise-Meitner-Straße 4 22941 Bargteheide Hierzu gilt die gesonderte Datenschutzvereinbarung der DVSE GmbH.

☒Außenstehende

Das Autohaus Kärgel gibt - ausser zu direkten Geschäftspartnern - keinerlei personenbezogene Daten an Dritte weiter außer bei Anfragen offizieller deutscher Ermittlungsbehörden.

☐Kinder

☒Sonstige

Nutzung des Cloud- und E-Mail Service der 1&1 Telecommunication SE Elgendorfer Str. 57 56410 Montabaur zur E-Mail Kommunikation und Dateiablage, insb. bez. Mitarbeitereinteilung / Schichtdienst / Einsatzpläne / Auftragsdaten. Hier gilt die

gesonderte Datenschutzverordnung der 1&1 Telecommunication SE
Nutzung der Placetel-Cloud-IP-Telefonanlage der BroadSoft Germany GmbH c/o Cisco Systems GmbH Lothringer Straße 56 D-50677 Köln
Hier gilt die gesonderte Datenschutzverordnung der BroadSoft Germany GmbH.

TOM-Checkliste für AMP Nr. 110272

1 Vertraulichkeit - Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Schließ- und Schlüsselsysteme

☒Manuelles Schließsystem
☐Elektronisches Schließsystem (z.B. Chipkarten, Transponder, Zutrittskarten usw.)
☒Schlüsselregelung und Protokollierung (Schlüsselausgabe etc.)
☒Sicherheitsschlösser
☐Sonstiges (bitte angeben):

Gebäudesicherheit

☐Fenstersicherung

☒Absicherung eines unberechtigten Zutritts über exponierte Gebäudeeinrichtungen (z.B. über Lüftungs-/Lichtschächte, Feuerleitern, Balkone etc.)
☐Einsatz von Wachpersonal
☐Lichtschranken/Bewegungsmelder
☐Videoüberwachung der Zugänge
☐Alarmanlage
☐Sonstiges (bitte angeben):

Personenkontrolle

☐Schriftliche Besucherregelung/Sicherstellung eines kontrollierten Aufenthalts externer Personen
☒Personenkontrolle beim Pförtner/Empfang
☐Protokollierung der Besucher (Nachvollziehbarkeit, wer ins Gebäude kommt)
☐Tragepflicht von Berechtigungsausweisen (Sicherstellung, dass ein berechtigter bzw. unberechtigter Aufenthalt erkannt wird)
☒Sorgfältige Auswahl von Reinigungspersonal
☒Überwachung von Wartungs- und Reinigungspersonal

Weiteres

☐Sonstige Maßnahmen zur Zutrittskontrolle:

2 Vertraulichkeit - Zugangskontrolle

Maßnahmen, die geeignet sind, das Eindringen Unbefugter in die DV-Systeme (IT-Systeme) zu verhindern.

Zugangssicherheit zu Datenverarbeitungssystemen

☒Benutzerprofile (Benutzerstammsätze) lassen sich eindeutig einer Person (User) zuordnen, wobei jeder User ein Benutzerprofil hat.
☒Zugangsrechte sind für die Mitarbeiter auf die Programme/Daten beschränkt, die sie auch verwenden müssen (individuelle Einrichtung von Zugangs- und Benutzerrechten)
☒Mitarbeiter erhalten Administratorenrechte nur, sofern es für Ihre Tätigkeit unabdingbar ist (restriktive Vergabe von Administrationsrechten)

Passwortsicherheit

☒Login mit Benutzerkennung und Passwort
☒Kennwortverfahren/Passwortregelungen (u.a. Sonderzeichen, Mindestlänge, regelmäßiger erzwungener Wechsel des Kennworts)
☐Automatische Sperrung eines Benutzers, wenn er das Passwort mehrmals

falsch eingibt sowie Regelungen für Folgemaßnahmen
☒Automatische Bildschirmsperren beim Verlassen des Arbeitsplatzes (Timeout)
IT- und Organisationssicherheit
☐Einsatz von VPN-Technologie
☒Organisatorische Vorkehrungen zur Verhinderung unberechtigter Zugriffe auf personenbezogene Daten am Arbeitsplatz (z.B. Richtlinien/Schulungen für Mitarbeiter)
☐Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum gezielten Löschen von Daten bei verlorengegangenen Smartphones)
☒Verschlüsselung von beweglichen Datenträgern (Laptops/Notebooks, USB Sticks, Smartphones etc.)
☒Einsatz einer Firewall (Hard- oder Software)

Weiteres
☐Sonstige Maßnahmen zur Zugangskontrolle:
3 Vertraulichkeit - Zugriffskontrolle
Maßnahmen, die geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Nutzerkontrolle in Datenverarbeitungssystemen und Berechtigungssicherheit
☒Benutzer besitzen nur Zugriffsberechtigungen auf Daten, die zur Ausübung ihrer Tätigkeit notwendig sind (Differenzierte Berechtigungen und Berechtigungskonzepte, z.B. Benutzerprofile, Rollen, begrenzter Zugriff auf Ordner)
☒Es ist sichergestellt, dass jede Person nur über ihr eigenes Benutzerprofil arbeiten kann (kein "Account-Sharing")
☒Verwaltung der Rechtevergabe in Datenverarbeitungssystemen durch System- bzw. IT-Administratoren (getrennte Verantwortlichkeiten, fachliche Eignung etc.)
☒Regelmäßige Kontrollen (z.B. durch Auswertungen/Reports der Zugriffe, Berechtigungsvergabe usw.)
Organisationssicherheit in Datenverarbeitungssystemen
☐Regelmäßige Prüfung und Bewertung von technisch-organisatorischen Maßnahmen um die Sicherheit der Verarbeitung zu gewährleisten, z.B. durch Penetrationstest (Pentests)
☒Absicherung von Fernwartungszugängen, Servern und Endgeräten, externer Schnittstellen
Datenlöschung und -vernichtung
☒Einsatz von datenschutzgerechten Aktenvernichtern bzw. Dienstleistern (Zertifizierung)
☒Ordnungsgemäße Vernichtung/Löschung von Datenträgern (z.B. Schreddern, DSGVO konformes Löschen nach z.B. BSI)
Weiteres
☒Sonstige Maßnahmen zur Zugriffskontrolle:
4 Integrität - Weitergabekontrolle
Maßnahmen, die geeignet sind, die Weitergabe personenbezogener Daten (elektronische Übertragung, Datentransport, Übermittlungskontrolle usw.) so zu regeln, dass ein Verlust, eine unbefugte/unbeabsichtigte Veränderung oder unbefugte Veröffentlichung verhindert werden. Maßnahmen, die hinsichtlich Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung getroffen wurden.
Protokollierung der Datenverarbeitung

☐Bestandsverzeichnis und Bestandskontrolle der Datenträger
☒Protokollierung der Empfänger von Daten
Verschlüsselungssicherheit und -möglichkeit bei Datenweitergabe
☒Verschlüsselte Plattformen zur Weitergabe von Daten
☒Verschlüsselte Datenübertragung bzw. Konzept für die Weitergabe von Daten

☐Verschlüsselung von Daten auf Datenträgern
☐E-Mail Verschlüsselung
Transportsicherheit bei Daten- bzw. Datenträgerweitergabe
☒Bei physischem Transport: sorgfältige Auswahl von Transportpersonal und -Fahrzeugen (z.B. Beauftragung von Kurieren und Dienstleistern, verschlossene Behälter)
Sicherstellung EU-Datenschutzniveau
☒Ist sichergestellt, dass die gesamte Verarbeitung der Daten nur innerhalb der EU stattfindet (inkl. Nutzung/Zugriff, eingesetzter Subauftragnehmer, Systemhosting, -wartung etc.)
☐Sofern die Datenverarbeitung außerhalb der EU stattfindet: Bitte erläutern und DSGVO entsprechende Garantien benennen, ggf. in einem eigenständigen Dokument
Weiteres
☐Sonstige Maßnahmen zur Weitergabekontrolle:
5 Integrität - Eingabekontrolle
Maßnahmen, die geeignet sind, die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege zu gewährleisten. Maßnahmen, die geeignet sind, die nachträgliche Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, zu gewährleisten.
Kontrollsicherheit bei Speicherung und Änderung von Daten
☒Protokollierungs- und Protokollauswertungssysteme bzgl. sämtlicher Systemaktivitäten (z.B. Jobprotokolle, Windows Ereignisprotokolle, Nagios usw.)
☐Datenschutzgerechte Aufbewahrung dieser Protokolle
Weiteres
☐Sonstige Maßnahmen zur Eingabekontrolle:
6 Auftragsverarbeitung - Auftragskontrolle
Maßnahmen, die geeignet sind, eine Auftragsdatenverarbeitung nach Art. 28 DSGVO zu gewährleisten. Dazu gelten gewisse Anforderungen (Weisungsgebundenheit, das Ergreifen von Maßnahmen nach Art. 32 DSGVO etc.)
Auftragnehmerauswahl und Vertragsmanagment
☐schriftliche Kriterien zur sorgfältigen Auswahl der Unterauftragnehmer
☐Klare vertragliche Regelungen (Aufgaben/ Verantwortung der Vertragspartner, DS Vereinbarungen etc.)
☒Abschluss von Auftragsverarbeitungsverträgen nach Art. 28 DSGVO mit schriftlicher Festlegung der Weisungsgebundenheit
☐Verzeichnis und Dokumentation von Auftragsverarbeitungsverträgen mit Dienstleistern
☒Kontrolle der Vertragsausführung (Kontrolle der Umsetzung der vertraglich vereinbarten Inhalte)
☒Überwachung / Kontrollen der Unterauftragnehmer (v.a. der technisch organisatorischen Maßnahmen)
☒Sicherstellung, dass die Verarbeitung der Daten entsprechend der Weisung des Auftraggebers beim Auftragnehmer (Unterauftragnehmer) erfolgt. Diese ist ausschießlich durch die damit betrauten Mitarbeiter durchzuführen (z.B.

durch Richtlinien, Arbeitsanweisungen, Zugriffssteuerung, Verpflichtung auf

Verschwiegenheit, etc.)
☐Anweisungen- und Richtlinien beim Vertragsmanagement
Weiteres
☐Sonstige Maßnahmen zur Auftragskontrolle:
7 Verfügbarkeitskontrolle
Maßnahmen, die geeignet sind, die Daten gegen zufällige Zerstörung oder Verlust zu schützen.
Getroffene Maßnahmen zur Datensicherung (physikalisch / logisch).
Datensicherung
☒Regelmäßige Datensicherungen/Backup-Verfahren von IT-Systemen
☐Sicherstellung der Ausfallsicherheit (z.B. RAID-Verfahren)
☒Getrennte und abgesicherte Aufbewahrung von Sicherungsdatenträgern (z.B. im Tresor, Bankschließfach, usw…)
Gebäudesicherheit / Serverräume
☒Server außerhalb des Unternehmens (Hosting, Cloud) Bitte Hoster incl. Sitz und Sicherheitsmaßnahmen / Garantien erläutern (ggf. in einem eigenständigen Dokument)
☒Gesicherte Serverräume (z.B. Serverräume befinden sich nicht unter sanitären Anlagen/Rohrleitungen, festes Mauerwerk, gesicherte Zugänge, Sicherheitsschlösser etc.)
☐Klimaanlage und Temperaturmessung in Serverräumen
☐Rauch- und Brandmelder, Sprinkleranlage, Brandschutztüren, Wasserschutzeinrichtungen etc.
☐Unterbrechungsfreie Stromversorgung (USV)
Interne Organisation bei Notfällen
☐Notfallplan (Disaster Recovery Plan)
☒Klare Meldewege bei Brand, Feuer oder Notfällen
Weiteres
☒Maßnahmen gegen Schadsoftware (z.B. Anti-Spy-Software/Spam-Filter/IDS oder IPS-Systeme)
☐Sonstige Maßnahmen zur Auftragskontrolle:
8 Vertraulichkeit / Trennungskontrolle
Maßnahmen, die geeignet sind, die getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke erhoben wurden sicherzustellen. Maßnahmen, die geeignet sind, die getrennten Verarbeitung der Daten unterschiedlicher Auftraggeber zu gewährleisten.
Verarbeitungskontrolle zu verschiedenen Zwecken
☒Detaillierte/ differenzierte Zugriffskonzepte
☐Einsatz von Testverfahren, die gewährleisten, dass keine personenbezogenen Daten zu Testzwecken verwendet werden (z.B. Anonymisierung von Testdaten)
Datentrennung
☒physische oder logische Trennung von Produktiv- und Testsystemen
☒Es ist sichergestellt, dass eine physisch bzw. logisch getrennten Speicherung und Verarbeitung von Daten umgesetzt ist (Mandantenfähigkeit, Mandantentrennung, z.B. getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)

Weiteres
☐Sonstige Maßnahmen zur Vertraulichkeit/Trennungskontrolle:
9 Organisationskontrolle
Maßnahmen, die geeignet sind, die reibungslose Organisation des Datenschutzes und der Sicherheit der Daten im Unternehmen sicherzustellen.
Datenschutzmanagement
☒Ein Datenschutzbeauftragter ist schriftlich benannt
☐Einschlägiges Datenschutz-Know-How ist im Unternehmen verfügbar (z.B. durch Schulungen, Zertifikat, Vertrag mit ext. Datenschutzberatung, etc.)

☒Regelmäßige Überprüfung, Bewertung und Evaluierung der technisch organisatorischen Maßnahmen auf Wirksamkeit (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

☒Regelmäßige Prüfung der internen Prozesse im Hinblick auf Datenschutz

☐Etabliertes Datenschutzmanagementsystem bzw. -systematik inkl. Prozess zur Sicherstellung von Betroffenenrechten

Unterweisung von Mitarbeitern und Organisation im Datenschutz

☐Regelmäßige Schulung der Mitarbeiter, Richtlinien/Handbücher bzw. Arbeitsanweisungen für die Mitarbeiter

☒Datenschutzmaßnahmen und Datenschutzinformationen bei der Einstellung sowie Kündigung von Mitarbeitern

☐IT-Richtlinie

☐schriftliche Regelungen für Telearbeit / Home Office

☒Verpflichtung (schriftlich) der Mitarbeiter auf das Datengeheimnis nach (Art. 28 Abs. 3 lit. b DSGVO)

Weiteres

☐Sonstige Maßnahmen zur Organisationskontrolle:

10 Risikoabschätzung

Welche risikobasierten Sicherungsmechanismen sind im Unternehmen etabliert? (vgl. Art. 32 DSGVO, Art. 25 DSGVO Abs. 1, Art. 35 DSGVO)

Risikoabschätzung / Datenschutzfolgenabschätzung (DSFA)

☒Durchführung von Risikoabschätzungen inkl. Festlegung geeigneter, technisch organisatorischer Maßnahmen

☒Durchführung von Datenschutzfolgeabschätzungen

☐Ist anhand der Risikoabschätzung/ DSFA eine Verschlüsselung, Pseudonymisierung oder Anonymisierung notwendig? Zutreffendes bitte erläutern.

☐Verschlüsselung der Daten bezüglich der Verarbeitung

☐Pseudonymisierung der Daten bezüglich der Verarbeitung

☐Anonymisierung der Daten bezüglich der Verarbeitung

11 Datenschutzmanagement

Wie ist das Datenschutzmanagmentsystem aufgestellt? z.B. Privacy by Design und Privacy by Default

Datenschutzorganisation

☒Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

☒Incident-Response-Management

☒Auftragskontrolle i.S.v. Art. 28 DSGVO

Weiteres

☐Sonstige Maßnahmen im Datenschutzmanagement:

12 Ergänzende oder erklärende Dokumente und/oder Zertifikate

Gibt es weitere Zertifikate, Sicherheitsmaßnahmen oder Kontrollprüfungsmechanismen, die Sie nachweisen können?

Zertifikate

☐ISO27001 Zertifikat, ISMS

☐Binding Corporate Rules (BCR)

☐TISAX Zertifikat

☐Sonstige Zertifikate

13 Ergänzende Maßnahmen

Bei speziellen Prozessen sind u.U. weitere Maßnahmen erforderlich - Notwendige Maßnahmen bitte ausführen

Annex 2 Nachweis Technische und organisatorische Maßnahmen (TOM) AMP Nr. 110574

Erläuterung: Die technischen und organisatorischen Maßnahmen (TOM) – und deren Dokumentation – sind das Herzstück des Datenschutzes eines

Unternehmens. Aus Art. 32 DSGVO ergibt sich die Verpflichtung eines Unternehmens, das selbst oder im Auftrag personenbezogene Daten verarbeitet, angemessene technische und organisatorische Maßnahmen umzusetzen und zu dokumentieren. Diese Anlage und vor allem Checkliste zu den technischen-organisatorischen Maßnahmen ist vom Auftragsverarbeiter zwingend entsprechend seiner innerbetrieblichen Organisation auszufüllen. Die innerbetriebliche Organisation ist vom Auftragsverarbeiter so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Bitte kreuzen Sie die Maßnahmen, welche zutreffen an und geben eine kurze Erläuterung dazu ab.

Eingesetzte Unterauftragnehmer bei AMP Nr. 110574

Nr. 1

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

Steuerberater Rieter und Schehl

Verarbeitete Datenkategorien

Abrechnungsdaten

Angaben zur Tätigkeit

Steuerberater

Ort der Datenverarbeitung

Bahnhofstr. 21, 76855 Annweiler

Nr. 2

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

Lawa Solutions

Verarbeitete Datenkategorien

Flotten-Management

Angaben zur Tätigkeit

Automobil-Logistik

Anlage 4 zum Rahmenvertrag Nr. 550001554

Annex 2 für AMP Nr. 110574 Seite A2-10

Ort der Datenverarbeitung

Zu den Mühlen 19, 35390 Giessen

Nr. 3

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

WM SE

Verarbeitete Datenkategorien

Ersatzteilbestellungen

Angaben zur Tätigkeit

Automobil-Ersatzteil Großhändler

Ort der Datenverarbeitung

Pagenstecherstraße 121 49090 Osnabrück

Art der verarbeiteten Daten bei AMP Nr. 110574

☒Berufliche Kontakt- und (Arbeits-)Organisationsdaten

Steuerberater: Bei Mitarbeitern, Name, Vorname, Anschrift, Personalnummern, Anwesenheit, Gehalt, Krankenkasse, Sozialversicherungsnummer, Vermögenswirksame Leistungen, bei Kunden und Lieferanten die Rechnungen / Belege, eigene Bankdaten Kontobewegungen, Kassenbuch

☒Daten zu beruflichen Verhältnissen

Steuerberater: Betriebszugehörigkeit, Aufgaben, Eintritts und Austritt, Tarifgruppe, Entgeltabrechnung, Sonderzahlungen, Pfändung, tägliche Anwesenheitszeiten, Abwesenheitsgründe,

☒Private Kontakt- und Identifikationsdaten

Steuerberater: Name, Vorname, Anschrift, Geburtsdatum/-ort, Identifikationsnummern, Kontoverbindungen

☐Vertragsdaten

☒Positionsdaten

Flottenmanagement: GPS, Bewegungsprofil der Betriebs Kfz, Fahrer,

Fahraufträge
☐Daten zu persönlichen Verhältnissen
☒Bonitäts- und Bankdaten
Steuerberater: Kontoverbindung, Kontobewegungen, Kassenbuch
☐Besonders sensible personenbezogene Daten
☒Sonstiges
Ersatzteilbestellungen und TÜV: Fahrzeugdaten teilweise inkl. Halterdaten und Kfz-Schein, Teile-Bestellungen, durchgeführte und durchzuführende Reparaturen.

Betroffene Personengruppen bei AMP Nr. 110574

☒Mitarbeiter des Auftraggebers/des Verantwortlichen
Nur zur Verschwiegenheit Verpflichtete Geschäftsinhaber, Teilhaber und Mitarbeiter
☐Mitarbeiter dritter Unternehmen
☒Kunden/ Mitglieder des Auftraggebers/ Verantwortlichen
Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110574 Seite A2-11
Mitarbeitern, Name, Vorname, Anschrift, Ausweisdaten, Führerscheindaten, Daten im Kfz-Schein, Angebote, Auftragsdaten, Rechnungsdaten
☒Sonstige Geschäftspartner
Die Administration der IT Systeme erfolgt extern durch Weis Consulting e.K., Zweibrücker Str. 35a, 66953 Pirmasens, www.weisconsulting.de. Verträge/AGBs gem. § 11 BDSG mit externen Dienstleistern liegen vor und können u.a. eingesehen werden u.a. unter http://www.weis-consulting.de/agb.htm. Die internen Abrechnungsdaten werden in der Datev Software verarbeitet. Hierzu gilt die gesonderte Datenschutzvereinbarung der Datev AG, Paumgarnterstr.6-14, 90329 Nürnberg, www.datev.de. Die Umsatzsteuererklärung wird mit Elster erledigt. Hier gilt die gesonderte Datenschutzverordnung der Deutschen Finanzverwaltung. Im Auftrag erfolgen eventuelle weitere Datenweitergaben, im Einvernehmen mit dem Kunden, an Kfz-Gutachter, die Stadtverwaltung, Versicherungen oder Rechtsanwälte. Die externe Rechnungsschreibung erfolgt durch KfzWin Software der DVSE Gesellschaft für Datenverarbeitung, Service und Entwicklung mbH Lise-Meitner-Straße 4 22941 Bargteheide Hierzu gilt die gesonderte Datenschutzvereinbarung der DVSE GmbH.
☒Außenstehende
Das Autohaus Kärgel gibt - ausser zu direkten Geschäftspartnern - keinerlei personenbezogene Daten an Dritte weiter außer bei Anfragen offizieller deutscher Ermittlungsbehörden.
☐Kinder
☒Sonstige
Nutzung des Cloud- und E-Mail Service der 1&1 Telecommunication SE Elgendorfer Str. 57 56410 Montabaur zur E-Mail Kommunikation und Dateiablage, insb. bez. Mitarbeitereinteilung / Schichtdienst / Einsatzpläne / Auftragsdaten. Hier gilt die gesonderte Datenschutzverordnung der 1&1 Telecommunication SE Nutzung der Placetel-Cloud-IP-Telefonanlage der BroadSoft Germany GmbH c/o Cisco Systems GmbH Lothringer Straße 56 D-50677 Köln Hier gilt die gesonderte Datenschutzverordnung der BroadSoft Germany GmbH.

TOM-Checkliste für AMP Nr. 110574

1 Vertraulichkeit - Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Schließ- und Schlüsselsysteme

☒Manuelles Schließsystem

☐Elektronisches Schließsystem (z.B. Chipkarten, Transponder, Zutrittskarten usw.)

☒Schlüsselregelung und Protokollierung (Schlüsselausgabe etc.)

☒Sicherheitsschlösser

☐Sonstiges (bitte angeben):

Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110574 Seite A2-12

Gebäudesicherheit

☐Fenstersicherung

☒Absicherung eines unberechtigten Zutritts über exponierte Gebäudeeinrichtungen (z.B. über Lüftungs-/Lichtschächte, Feuerleitern, Balkone etc.)

☐Einsatz von Wachpersonal

☐Lichtschranken/Bewegungsmelder

☐Videoüberwachung der Zugänge

☐Alarmanlage

☐Sonstiges (bitte angeben):

Personenkontrolle

☐Schriftliche Besucherregelung/Sicherstellung eines kontrollierten Aufenthalts externer Personen

☒Personenkontrolle beim Pförtner/Empfang

☐Protokollierung der Besucher (Nachvollziehbarkeit, wer ins Gebäude kommt)

☐Tragepflicht von Berechtigungsausweisen (Sicherstellung, dass ein berechtigter bzw. unberechtigter Aufenthalt erkannt wird)

☒Sorgfältige Auswahl von Reinigungspersonal

☒Überwachung von Wartungs- und Reinigungspersonal

Weiteres

☐Sonstige Maßnahmen zur Zutrittskontrolle:

2 Vertraulichkeit - Zugangskontrolle

Maßnahmen, die geeignet sind, das Eindringen Unbefugter in die DV-Systeme (IT-Systeme) zu verhindern.

Zugangssicherheit zu Datenverarbeitungssystemen

☒Benutzerprofile (Benutzerstammsätze) lassen sich eindeutig einer Person (User) zuordnen, wobei jeder User ein Benutzerprofil hat.

☒Zugangsrechte sind für die Mitarbeiter auf die Programme/Daten beschränkt, die sie auch verwenden müssen (individuelle Einrichtung von Zugangs- und Benutzerrechten)

☒Mitarbeiter erhalten Administratorenrechte nur, sofern es für Ihre Tätigkeit unabdingbar ist (restriktive Vergabe von Administrationsrechten)

Passwortsicherheit

☒Login mit Benutzerkennung und Passwort

☒Kennwortverfahren/Passwortregelungen (u.a. Sonderzeichen, Mindestlänge, regelmäßiger erzwungener Wechsel des Kennworts)

☐Automatische Sperrung eines Benutzers, wenn er das Passwort mehrmals falsch eingibt sowie Regelungen für Folgemaßnahmen

☒Automatische Bildschirmsperren beim Verlassen des Arbeitsplatzes (Timeout)

IT- und Organisationssicherheit

☐Einsatz von VPN-Technologie

☒Organisatorische Vorkehrungen zur Verhinderung unberechtigter Zugriffe auf personenbezogene Daten am Arbeitsplatz (z.B. Richtlinien/Schulungen für Mitarbeiter)

☐Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum gezielten Löschen von Daten bei verlorengegangenen Smartphones)

☒Verschlüsselung von beweglichen Datenträgern (Laptops/Notebooks, USB Sticks, Smartphones etc.)
☒Einsatz einer Firewall (Hard- oder Software)

Weiteres

☐Sonstige Maßnahmen zur Zugangskontrolle:

3 Vertraulichkeit - Zugriffskontrolle

Maßnahmen, die geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Nutzerkontrolle in Datenverarbeitungssystemen und Berechtigungssicherheit

☒Benutzer besitzen nur Zugriffsberechtigungen auf Daten, die zur Ausübung ihrer Tätigkeit notwendig sind (Differenzierte Berechtigungen und Berechtigungskonzepte, z.B. Benutzerprofile, Rollen, begrenzter Zugriff auf Ordner)
☒Es ist sichergestellt, dass jede Person nur über ihr eigenes Benutzerprofil arbeiten kann (kein "Account-Sharing")
☒Verwaltung der Rechtevergabe in Datenverarbeitungssystemen durch System- bzw. IT-Administratoren (getrennte Verantwortlichkeiten, fachliche Eignung etc.)
☒Regelmäßige Kontrollen (z.B. durch Auswertungen/Reports der Zugriffe, Berechtigungsvergabe usw.)

Organisationssicherheit in Datenverarbeitungssystemen

☐Regelmäßige Prüfung und Bewertung von technisch-organisatorischen Maßnahmen um die Sicherheit der Verarbeitung zu gewährleisten, z.B. durch Penetrationstest (Pentests)
☒Absicherung von Fernwartungszugängen, Servern und Endgeräten, externer Schnittstellen

Datenlöschung und -vernichtung

☒Einsatz von datenschutzgerechten Aktenvernichtern bzw. Dienstleistern (Zertifizierung)
☒Ordnungsgemäße Vernichtung/Löschung von Datenträgern (z.B. Schreddern, DSGVO konformes Löschen nach z.B. BSI)

Weiteres

☒Sonstige Maßnahmen zur Zugriffskontrolle:

4 Integrität - Weitergabekontrolle

Maßnahmen, die geeignet sind, die Weitergabe personenbezogener Daten (elektronische Übertragung, Datentransport, Übermittlungskontrolle usw.) so zu regeln, dass ein Verlust, eine unbefugte/unbeabsichtigte Veränderung oder unbefugte Veröffentlichung verhindert werden. Maßnahmen, die hinsichtlich Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung getroffen wurden.

Protokollierung der Datenverarbeitung

☐Bestandsverzeichnis und Bestandskontrolle der Datenträger
☒Protokollierung der Empfänger von Daten

Verschlüsselungssicherheit und -möglichkeit bei Datenweitergabe

☒Verschlüsselte Plattformen zur Weitergabe von Daten
☒Verschlüsselte Datenübertragung bzw. Konzept für die Weitergabe von Daten
☐Verschlüsselung von Daten auf Datenträgern
☐E-Mail Verschlüsselung

Transportsicherheit bei Daten- bzw. Datenträgerweitergabe

☒Bei physischem Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen (z.B. Beauftragung von Kurieren und Dienstleistern, verschlossene Behälter)

Sicherstellung EU-Datenschutzniveau

☒Ist sichergestellt, dass die gesamte Verarbeitung der Daten nur innerhalb der EU stattfindet (inkl. Nutzung/Zugriff, eingesetzter Subauftragnehmer, Systemhosting, -wartung etc.)

☐Sofern die Datenverarbeitung außerhalb der EU stattfindet: Bitte erläutern und DSGVO entsprechende Garantien benennen, ggf. in einem eigenständigen Dokument

Weiteres

☐Sonstige Maßnahmen zur Weitergabekontrolle:

5 Integrität - Eingabekontrolle

Maßnahmen, die geeignet sind, die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege zu gewährleisten. Maßnahmen, die geeignet sind, die nachträgliche Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, zu gewährleisten.

Kontrollsicherheit bei Speicherung und Änderung von Daten

☒Protokollierungs- und Protokollauswertungssysteme bzgl. sämtlicher Systemaktivitäten (z.B. Jobprotokolle, Windows Ereignisprotokolle, Nagios usw.)

☐Datenschutzgerechte Aufbewahrung dieser Protokolle

Weiteres

☐Sonstige Maßnahmen zur Eingabekontrolle:

6 Auftragsverarbeitung - Auftragskontrolle

Maßnahmen, die geeignet sind, eine Auftragsdatenverarbeitung nach Art. 28 DSGVO zu gewährleisten. Dazu gelten gewisse Anforderungen (Weisungsgebundenheit, das Ergreifen von Maßnahmen nach Art. 32 DSGVO etc.)

Auftragnehmerauswahl und Vertragsmanagment

☐schriftliche Kriterien zur sorgfältigen Auswahl der Unterauftragnehmer

☐Klare vertragliche Regelungen (Aufgaben/ Verantwortung der Vertragspartner, DS Vereinbarungen etc.)

☒Abschluss von Auftragsverarbeitungsverträgen nach Art. 28 DSGVO mit schriftlicher Festlegung der Weisungsgebundenheit

☐Verzeichnis und Dokumentation von Auftragsverarbeitungsverträgen mit Dienstleistern

☒Kontrolle der Vertragsausführung (Kontrolle der Umsetzung der vertraglich vereinbarten Inhalte)

☒Überwachung / Kontrollen der Unterauftragnehmer (v.a. der technisch organisatorischen Maßnahmen)

☒Sicherstellung, dass die Verarbeitung der Daten entsprechend der Weisung des Auftraggebers beim Auftragnehmer (Unterauftragnehmer) erfolgt. Diese ist ausschießlich durch die damit betrauten Mitarbeiter durchzuführen (z.B. durch Richtlinien, Arbeitsanweisungen, Zugriffssteuerung, Verpflichtung auf Verschwiegenheit, etc.)

☐Anweisungen- und Richtlinien beim Vertragsmanagement

Weiteres

☐Sonstige Maßnahmen zur Auftragskontrolle:

7 Verfügbarkeitskontrolle

Maßnahmen, die geeignet sind, die Daten gegen zufällige Zerstörung oder Verlust zu schützen. Getroffene Maßnahmen zur Datensicherung (physikalisch / logisch).

Datensicherung

☒Regelmäßige Datensicherungen/Backup-Verfahren von IT-Systemen

☐Sicherstellung der Ausfallsicherheit (z.B. RAID-Verfahren)

☒Getrennte und abgesicherte Aufbewahrung von Sicherungsdatenträgern (z.B. im Tresor, Bankschließfach, usw…)

Gebäudesicherheit / Serverräume

☒Server außerhalb des Unternehmens (Hosting, Cloud) Bitte Hoster incl. Sitz und Sicherheitsmaßnahmen / Garantien erläutern (ggf. in einem eigenständigen Dokument)

☒Gesicherte Serverräume (z.B. Serverräume befinden sich nicht unter sanitären Anlagen/Rohrleitungen, festes Mauerwerk, gesicherte Zugänge, Sicherheitsschlösser etc.)

☐Klimaanlage und Temperaturmessung in Serverräumen

☐Rauch- und Brandmelder, Sprinkleranlage, Brandschutztüren, Wasserschutzeinrichtungen etc.

☐Unterbrechungsfreie Stromversorgung (USV)

Interne Organisation bei Notfällen

☐Notfallplan (Disaster Recovery Plan)

☒Klare Meldewege bei Brand, Feuer oder Notfällen

Weiteres

☒Maßnahmen gegen Schadsoftware (z.B. Anti-Spy-Software/Spam-Filter/IDS oder IPS-Systeme)

☐Sonstige Maßnahmen zur Auftragskontrolle:

8 Vertraulichkeit / Trennungskontrolle

Maßnahmen, die geeignet sind, die getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke erhoben wurden sicherzustellen. Maßnahmen, die geeignet sind, die getrennten Verarbeitung der Daten unterschiedlicher Auftraggeber zu gewährleisten.

Verarbeitungskontrolle zu verschiedenen Zwecken

☒Detaillierte/ differenzierte Zugriffskonzepte

☐Einsatz von Testverfahren, die gewähleisten, dass keine personenbezogenen Daten zu Testzwecken verwendet werden (z.B. Anonymisierung von Testdaten)

Datentrennung

☒physische oder logische Trennung von Produktiv- und Testsystemen

☒Es ist sichergestellt, dass eine physisch bzw. logisch getrennten Speicherung und Verarbeitung von Daten umgesetzt ist (Mandantenfähigkeit, Mandantentrennung, z.B. getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)

Weiteres

☐Sonstige Maßnahmen zur Vertraulichkeit/Trennungskontrolle:

9 Organisationskontrolle

Maßnahmen, die geeignet sind, die reibungslose Organisation des Datenschutzes und der Sicherheit der Daten im Unternehmen sicherzustellen.

Datenschutzmanagement

☒Ein Datenschutzbeauftragter ist schriftlich benannt

☐Einschlägiges Datenschutz-Know How ist im Unternehmen verfügbar (z.B. durch Schulungen, Zertifikat, Vertrag mit ext. Datenschutzberatung, etc.)

☒Regelmäßige Überprüfung, Bewertung und Evaluierung der technisch organisatorischen Maßnahmen auf Wirksamkeit (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

☒Regelmäßige Prüfung der internen Prozesse im Hinblick auf Datenschutz

☐Etabliertes Datenschutzmanagementsystem bzw. -systematik inkl. Prozess zur Sicherstellung von Betroffenenrechten

Unterweisung von Mitarbeitern und Organisation im Datenschutz

☐Regelmäßige Schulung der Mitarbeiter, Richtlinien/Handbücher bzw. Arbeitsanweisungen für die Mitarbeiter

☒Datenschutzmaßnahmen und Datenschutzinformationen bei der Einstellung sowie Kündigung von Mitarbeitern

☐IT-Richtlinie

☐schriftliche Regelungen für Telearbeit / Home Office

☒Verpflichtung (schriftlich) der Mitarbeiter auf das Datengeheimnis nach (Art. 28 Abs. 3 lit. b DSGVO)

Weiteres

☐Sonstige Maßnahmen zur Organisationskontrolle:

10 Risikoabschätzung

Welche risikobasierten Sicherungsmechanismen sind im Unternehmen etabliert? (vgl. Art. 32 DSGVO, Art. 25 DSGVO Abs. 1, Art. 35 DSGVO)

Risikoabschätzung / Datenschutzfolgenabschätzung (DSFA)

☒Durchführung von Risikoabschätzungen inkl. Festlegung geeigneter, technisch organisatorischer Maßnahmen

☒Durchführung von Datenschutzfolgeabschätzungen

☐Ist anhand der Risikoabschätzung/ DSFA eine Verschlüsselung, Pseudonymisierung oder Anonymisierung notwendig? Zutreffendes bitte erläutern.

☐Verschlüsselung der Daten bezüglich der Verarbeitung

☐Pseudonymisierung der Daten bezüglich der Verarbeitung

☐Anonymisierung der Daten bezüglich der Verarbeitung

11 Datenschutzmanagement

Wie ist das Datenschutzmanagmentsystem aufgestellt? z.B. Privacy by Design und Privacy by Default

Datenschutzorganisation

☒Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

☒Incident-Response-Management

☒Auftragskontrolle i.S.v. Art. 28 DSGVO

Weiteres

☐Sonstige Maßnahmen im Datenschutzmanagement:

12 Ergänzende oder erklärende Dokumente und/oder Zertifikate

Gibt es weitere Zertifikate, Sicherheitsmaßnahmen oder Kontrollprüfungsmechanismen, die Sie nachweisen können?

Zertifikate

☐ISO27001 Zertifikat, ISMS

☐Binding Corporate Rules (BCR)

☐TISAX Zertifikat

☐Sonstige Zertifikate

13 Ergänzende Maßnahmen

Bei speziellen Prozessen sind u.U. weitere Maßnahmen erforderlich - Notwendige Maßnahmen bitte ausführen

Annex 2 Nachweis Technische und organisatorische Maßnahmen (TOM) AMP Nr. 110604

Erläuterung: Die technischen und organisatorischen Maßnahmen (TOM) – und deren Dokumentation – sind das Herzstück des Datenschutzes eines Unternehmens. Aus Art. 32 DSGVO ergibt sich die Verpflichtung eines Unternehmens, das selbst oder im Auftrag personenbezogene Daten verarbeitet, angemessene technische und organisatorische Maßnahmen umzusetzen und zu dokumentieren. Diese Anlage und vor allem Checkliste zu den technischen-organisatorischen Maßnahmen ist vom Auftragsverarbeiter zwingend entsprechend seiner innerbetrieblichen Organisation auszufüllen. Die innerbetriebliche Organisation ist vom Auftragsverarbeiter so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Bitte kreuzen Sie die Maßnahmen, welche zutreffen an und geben eine kurze

Erläuterung dazu ab.

Eingesetzte Unterauftragnehmer bei AMP Nr. 110604

Nr. 1

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

Steuerberater Rieter und Schehl

Verarbeitete Datenkategorien

Abrechnungsdaten

Angaben zur Tätigkeit

Steuerberater

Ort der Datenverarbeitung

Bahnhofstr. 21, 76855 Annweiler

Nr. 2

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

Lawa Solutions
Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110604 Seite A2-18

Verarbeitete Datenkategorien

Flotten-Management

Angaben zur Tätigkeit

Automobil-Logistik

Ort der Datenverarbeitung

Zu den Mühlen 19, 35390 Giessen

Nr. 3

Unterauftragnehmer (Name, Anschrift, Ansprechpartner)

WM SE

Verarbeitete Datenkategorien

Ersatzteilbestellungen

Angaben zur Tätigkeit

Automobil-Ersatzteil Großhändler

Ort der Datenverarbeitung

Pagenstecherstraße 121 49090 Osnabrück

Art der verarbeiteten Daten bei AMP Nr. 110604

☒Berufliche Kontakt- und (Arbeits-)Organisationsdaten
Steuerberater: Bei Mitarbeitern, Name, Vorname, Anschrift, Personalnummern, Anwesenheit, Gehalt, Krankenkasse, Sozialversicherungsnummer, Vermögenswirksame Leistungen, bei Kunden und Lieferanten die Rechnungen / Belege, eigene Bankdaten Kontobewegungen, Kassenbuch

☒Daten zu beruflichen Verhältnissen
Steuerberater: Betriebszugehörigkeit, Aufgaben, Eintrittsund Austritt, Tarifgruppe, Entgeltabrechnung, Sonderzahlungen, Pfändung, tägliche Anwesenheitszeiten, Abwesenheitsgründe,

☒Private Kontakt- und Identifikationsdaten
Steuerberater: Name, Vorname, Anschrift, Geburtsdatum/-ort, Identifikationsnummern, Kontoverbindungen

☐Vertragsdaten

☒Positionsdaten
Flottenmanagement: GPS, Bewegungsprofil der Betriebs Kfz, Fahrer, Fahraufträge

☐Daten zu persönlichen Verhältnissen

☒Bonitäts- und Bankdaten
Steuerberater: Kontoverbindung, Kontobewegungen, Kassenbuch

☐Besonders sensible personenbezogene Daten

☒Sonstiges
Ersatzteilbestellungen und TÜV: Fahrzeugdaten teilweise inkl. Halterdaten und kfzSchein, Teile-Bestellungen, durchgeführte und durchzuführende Reparaturen.

Betroffene Personengruppen bei AMP Nr. 110604

☒Mitarbeiter des Auftraggebers/des Verantwortlichen
Nur zur Verschwiegenheit Verpflichtete Geschäftsinhaber,
Teilhaber und Mitarbeiter
Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110604 Seite A2-19

☐Mitarbeiter dritter Unternehmen

☒Kunden/ Mitglieder des Auftraggebers/ Verantwortlichen
Mitarbeitern, Name, Vorname, Anschrift, Ausweisdaten,
Führerscheindaten, Daten im Kfz-Schein, Angebote, Auftragsdaten,
Rechnungsdaten

☒Sonstige Geschäftspartner
Die Administration der IT Systeme erfolgt extern durch Weis
Consulting e.K., Zweibrücker Str. 35a, 66953 Pirmasens, www.weisconsulting.
de. Verträge/AGBs gem. § 11 BDSG mit externen
Dienstleistern liegen vor und können u.a. eingesehen werden
u.a. unter http://www.weis-consulting.de/agb.htm. Die internen
Abrechnungsdaten werden in der Datev Software verarbeitet.
Hierzu gilt die gesonderte Datenschutzvereinbarung der Datev
AG, Paumgarnterstr.6-14, 90329 Nürnberg, www.datev.de. Die
Umsatzsteuererklärung wird mit Elster erledigt. Hier gilt die
gesonderte Datenschutzverordnung der Deutschen Finanzverwaltung.
Im Auftrag erfolgen eventuelle weitere Datenweitergaben,
im Einvernehmen mit dem Kunden, an Kfz-Gutachter, die
Stadtverwaltung, Versicherungen oder Rechtsanwälte. Die externe
Rechnungsschreibung erfolgt durch KfzWin Software der DVSE
Gesellschaft für Datenverarbeitung, Service und Entwicklung
mbH Lise-Meitner-Straße 4 22941 Bargteheide Hierzu gilt die
gesonderte Datenschutzvereinbarung der DVSE GmbH.

☒Außenstehende
Das Autohaus Kärgel gibt - ausser zu direkten Geschäftspartnern
- keinerlei personenbezogene Daten an Dritte weiter außer bei
Anfragen offizieller deutscher Ermittlungsbehörden.

☐Kinder

☒Sonstige
Nutzung des Cloud- und E-Mail Service der 1&1 Telecommunication
SE Elgendorfer Str. 57 56410 Montabaur zur E-Mail Kommunikation
und Dateiablage, insb. bez. Mitarbeitereinteilung /
Schichtdienst / Einsatzpläne / Auftragsdaten. Hier gilt die
gesonderte Datenschutzverordnung der 1&1 Telecommunication SE
Nutzung der Placetel-Cloud-IP-Telefonanlage der BroadSoft Germany
GmbH c/o Cisco Systems GmbH Lothringer Straße 56 D-50677 Köln
Hier gilt die gesonderte Datenschutzverordnung der BroadSoft
Germany GmbH.

TOM-Checkliste für AMP Nr. 110604

1 Vertraulichkeit - Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Schließ- und Schlüsselsysteme

☒Manuelles Schließsystem

☐Elektronisches Schließsystem (z.B. Chipkarten, Transponder, Zutrittskarten
usw.)

☒Schlüsselregelung und Protokollierung (Schlüsselausgabe etc.)
Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110604 Seite A2-20

☒Sicherheitsschlösser

☐Sonstiges (bitte angeben):

Gebäudesicherheit

☐Fenstersicherung

☒Absicherung eines unberechtigten Zutritts über exponierte Gebäudeeinrichtungen (z.B. über Lüftungs-/Lichtschächte, Feuerleitern, Balkone etc.)

☐Einsatz von Wachpersonal

☐Lichtschranken/Bewegungsmelder

☒Videoüberwachung der Zugänge

☐Alarmanlage

☐Sonstiges (bitte angeben):

Personenkontrolle

☐Schriftliche Besucherregelung/Sicherstellung eines kontrollierten Aufenthalts externer Personen

☒Personenkontrolle beim Pförtner/Empfang

☐Protokollierung der Besucher (Nachvollziehbarkeit, wer ins Gebäude kommt)

☐Tragepflicht von Berechtigungsausweisen (Sicherstellung, dass ein berechtigter bzw. unberechtigter Aufenthalt erkannt wird)

☒Sorgfältige Auswahl von Reinigungspersonal

☒Überwachung von Wartungs- und Reinigungspersonal

Weiteres

☐Sonstige Maßnahmen zur Zutrittskontrolle:

2 Vertraulichkeit - Zugangskontrolle

Maßnahmen, die geeignet sind, das Eindringen Unbefugter in die DV-Systeme (IT-Systeme) zu verhindern.

Zugangssicherheit zu Datenverarbeitungssystemen

☒Benutzerprofile (Benutzerstammsätze) lassen sich eindeutig einer Person (User) zuordnen, wobei jeder User ein Benutzerprofil hat.

☒Zugangsrechte sind für die Mitarbeiter auf die Programme/Daten beschränkt, die sie auch verwenden müssen (individuelle Einrichtung von Zugangs- und Benutzerrechten)

☒Mitarbeiter erhalten Administratorenrechte nur, sofern es für Ihre Tätigkeit unabdingbar ist (restriktive Vergabe von Administrationsrechten)

Passwortsicherheit

☒Login mit Benutzerkennung und Passwort

☒Kennwortverfahren/Passwortregelungen (u.a. Sonderzeichen, Mindestlänge, regelmäßiger erzwungener Wechsel des Kennworts)

☐Automatische Sperrung eines Benutzers, wenn er das Passwort mehrmals falsch eingibt sowie Regelungen für Folgemaßnahmen

☒Automatische Bildschirmsperren beim Verlassen des Arbeitsplatzes (Timeout)

IT- und Organisationssicherheit

☐Einsatz von VPN-Technologie

☒Organisatorische Vorkehrungen zur Verhinderung unberechtigter Zugriffe auf personenbezogene Daten am Arbeitsplatz (z.B. Richtlinien/Schulungen für Mitarbeiter)

☐Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum gezielten Löschen von Daten bei verlorengegangenen Smartphones)

☒Verschlüsselung von beweglichen Datenträgern (Laptops/Notebooks, USB Sticks, Smartphones etc.)

☒Einsatz einer Firewall (Hard- oder Software)

Weiteres

☐Sonstige Maßnahmen zur Zugangskontrolle:

3 Vertraulichkeit - Zugriffskontrolle

Maßnahmen, die geeignet sind, zu gewährleisten, dass die zur Benutzung eines

Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Nutzerkontrolle in Datenverarbeitungssystemen und Berechtigungssicherheit

☒Benutzer besitzen nur Zugriffsberechtigungen auf Daten, die zur Ausübung ihrer Tätigkeit notwendig sind (Differenzierte Berechtigungen und Berechtigungskonzepte, z.B. Benutzerprofile, Rollen, begrenzter Zugriff auf Ordner)

☒Es ist sichergestellt, dass jede Person nur über ihr eigenes Benutzerprofil arbeiten kann (kein "Account-Sharing")

☒Verwaltung der Rechtevergabe in Datenverarbeitungssystemen durch System- bzw. IT-Administratoren (getrennte Verantwortlichkeiten, fachliche Eignung etc.)

☒Regelmäßige Kontrollen (z.B. durch Auswertungen/Reports der Zugriffe, Berechtigungsvergabe usw.)

Organisationssicherheit in Datenverarbeitungssystemen

☐Regelmäßige Prüfung und Bewertung von technisch-organisatorischen Maßnahmen um die Sicherheit der Verarbeitung zu gewährleisten, z.B. durch Penetrationstest (Pentests)

☒Absicherung von Fernwartungszugängen, Servern und Endgeräten, externer Schnittstellen

Datenlöschung und -vernichtung

☒Einsatz von datenschutzgerechten Aktenvernichtern bzw. Dienstleistern (Zertifizierung)

☒Ordnungsgemäße Vernichtung/Löschung von Datenträgern (z.B. Schreddern, DSGVO konformes Löschen nach z.B. BSI)

Weiteres

☒Sonstige Maßnahmen zur Zugriffskontrolle:

4 Integrität - Weitergabekontrolle

Maßnahmen, die geeignet sind, die Weitergabe personenbezogener Daten (elektronische Übertragung, Datentransport, Übermittlungskontrolle usw.) so zu regeln, dass ein Verlust, eine unbefugte/unbeabsichtigte Veränderung oder unbefugte Veröffentlichung verhindert werden. Maßnahmen, die hinsichtlich Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung getroffen wurden.

Protokollierung der Datenverarbeitung

☐Bestandsverzeichnis und Bestandskontrolle der Datenträger

☒Protokollierung der Empfänger von Daten

Verschlüsselungssicherheit und -möglichkeit bei Datenweitergabe

☒Verschlüsselte Plattformen zur Weitergabe von Daten

☒Verschlüsselte Datenübertragung bzw. Konzept für die Weitergabe von Daten

☐Verschlüsselung von Daten auf Datenträgern

☐E-Mail-Verschlüsselung

Transportsicherheit bei Daten- bzw. Datenträgerweitergabe

☒Bei physischem Transport: sorgfältige Auswahl von Transportpersonal und -Fahrzeugen (z.B. Beauftragung von Kurieren und Dienstleistern, verschlossene Behälter)

Sicherstellung EU-Datenschutzniveau

☒Ist sichergestellt, dass die gesamte Verarbeitung der Daten nur innerhalb der EU stattfindet (inkl. Nutzung/Zugriff, eingesetzter Subauftragnehmer, Systemhosting, -wartung etc.)

☐Sofern die Datenverarbeitung außerhalb der EU stattfindet: Bitte

erläutern und DSGVO entsprechende Garantien benennen, ggf. in einem eigenständigen Dokument

Weiteres

☐Sonstige Maßnahmen zur Weitergabekontrolle:

5 Integrität - Eingabekontrolle

Maßnahmen, die geeignet sind, die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege zu gewährleisten. Maßnahmen, die geeignet sind, die nachträgliche Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, zu gewährleisten.

Kontrollsicherheit bei Speicherung und Änderung von Daten

☒Protokollierungs- und Protokollauswertungssysteme bzgl. sämtlicher Systemaktivitäten (z.B. Jobprotokolle, Windows Ereignisprotokolle, Nagios usw.)

☐Datenschutzgerechte Aufbewahrung dieser Protokolle

Weiteres

☐Sonstige Maßnahmen zur Eingabekontrolle:

6 Auftragsverarbeitung - Auftragskontrolle

Maßnahmen, die geeignet sind, eine Auftragsdatenverarbeitung nach Art. 28 DSGVO zu gewährleisten. Dazu gelten gewisse Anforderungen (Weisungsgebundenheit, das Ergreifen von Maßnahmen nach Art. 32 DSGVO etc.)

Auftragnehmerauswahl und Vertragsmanagment

☐schriftliche Kriterien zur sorgfältigen Auswahl der Unterauftragnehmer

☐Klare vertragliche Regelungen (Aufgaben/ Verantwortung der Vertragspartner, DS Vereinbarungen etc.)

☒Abschluss von Auftragsverarbeitungsverträgen nach Art. 28 DSGVO mit schriftlicher Festlegung der Weisungsgebundenheit

☐Verzeichnis und Dokumentation von Auftragsverarbeitungsverträgen mit Dienstleistern

☒Kontrolle der Vertragsausführung (Kontrolle der Umsetzung der vertraglich vereinbarten Inhalte)

☒Überwachung / Kontrollen der Unterauftragnehmer (v.a. der technisch organisatorischen Maßnahmen)

☒Sicherstellung, dass die Verarbeitung der Daten entsprechend der Weisung des Auftraggebers beim Auftragnehmer (Unterauftragnehmer) erfolgt. Diese ist ausschießlich durch die damit betrauten Mitarbeiter durchzuführen (z.B. durch Richtlinien, Arbeitsanweisungen, Zugriffssteuerung, Verpflichtung auf Verschwiegenheit, etc.)

☐Anweisungen- und Richtlinien beim Vertragsmanagement

Weiteres

☐Sonstige Maßnahmen zur Auftragskontrolle:

7 Verfügbarkeitskontrolle

Maßnahmen, die geeignet sind, die Daten gegen zufällige Zerstörung oder Verlust zu schützen. Getroffene Maßnahmen zur Datensicherung (physikalisch / logisch).

Datensicherung

☒Regelmäßige Datensicherungen/Backup-Verfahren von IT-Systemen

☐Sicherstellung der Ausfallsicherheit (z.B. RAID-Verfahren)

☒Getrennte und abgesicherte Aufbewahrung von Sicherungsdatenträgern (z.B. im Tresor, Bankschließfach, usw…)

Gebäudesicherheit / Serverräume

☒Server außerhalb des Unternehmens (Hosting, Cloud) Bitte Hoster incl. Sitz und Sicherheitsmaßnahmen / Garantien erläutern (ggf. in einem eigenständigen Dokument)

☒Gesicherte Serverräume (z.B. Serverräume befinden sich nicht unter sanitären Anlagen/Rohrleitungen, festes Mauerwerk, gesicherte Zugänge,

Sicherheitsschlösser etc.)
☐Klimaanlage und Temperaturmessung in Serverräumen
☐Rauch- und Brandmelder, Sprinkleranlage, Brandschutztüren, Wasserschutzeinrichtungen etc.
☐Unterbrechungsfreie Stromversorgung (USV)

Interne Organisation bei Notfällen

☐Notfallplan (Disaster Recovery Plan)
☒Klare Meldewege bei Brand, Feuer oder Notfällen

Weiteres

☒Maßnahmen gegen Schadsoftware (z.B. Anti-Spy-Software/Spam-Filter/IDS oder IPS-Systeme)
☐Sonstige Maßnahmen zur Auftragskontrolle:

8 Vertraulichkeit / Trennungskontrolle

Maßnahmen, die geeignet sind, die getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke erhoben wurden sicherzustellen. Maßnahmen, die geeignet sind, die getrennten Verarbeitung der Daten unterschiedlicher Auftraggeber zu gewährleisten.

Verarbeitungskontrolle zu verschiedenen Zwecken

☒Detaillierte/ differenzierte Zugriffskonzepte
☐Einsatz von Testverfahren, die gewährleisten, dass keine personenbezogenen Daten zu Testzwecken verwendet werden (z.B. Anonymisierung von Testdaten)

Datentrennung

☒physische oder logische Trennung von Produktiv- und Testsystemen
☒Es ist sichergestellt, dass eine physisch bzw. logisch getrennten Speicherung und Verarbeitung von Daten umgesetzt ist (Mandantenfähigkeit, Mandantentrennung, z.B. getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)

Weiteres

☐Sonstige Maßnahmen zur Vertraulichkeit/Trennungskontrolle:

9 Organisationskontrolle

Maßnahmen, die geeignet sind, die reibungslose Organisation des Datenschutzes und der Sicherheit der Daten im Unternehmen sicherzustellen.

Datenschutzmanagement

☒Ein Datenschutzbeauftragter ist schriftlich benannt
☐Einschlägiges Datenschutz-Know-How ist im Unternehmen verfügbar (z.B. durch Schulungen, Zertifikat, Vertrag mit ext. Datenschutzberatung, etc.)
☒Regelmäßige Überprüfung, Bewertung und Evaluierung der technisch organisatorischen Maßnahmen auf Wirksamkeit (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
☒Regelmäßige Prüfung der internen Prozesse im Hinblick auf Datenschutz
☐Etabliertes Datenschutzmanagementsystem bzw. -systematik inkl. Prozess zur Sicherstellung von Betroffenenrechten

Unterweisung von Mitarbeitern und Organisation im Datenschutz

☐Regelmäßige Schulung der Mitarbeiter, Richtlinien/Handbücher bzw. Arbeitsanweisungen für die Mitarbeiter
☒Datenschutzmaßnahmen und Datenschutzinformationen bei der Einstellung sowie Kündigung von Mitarbeitern
☐IT-Richtlinie
☐schriftliche Regelungen für Telearbeit / Home Office
☒Verpflichtung (schriftlich) der Mitarbeiter auf das Datengeheimnis nach (Art. 28 Abs. 3 lit. b DSGVO)

Weiteres

☐Sonstige Maßnahmen zur Organisationskontrolle:

10 Risikoabschätzung

Welche risikobasierten Sicherungsmechanismen sind im Unternehmen etabliert? (vgl. Art. 32 DSGVO, Art. 25 DSGVO Abs. 1, Art. 35 DSGVO)

Risikoabschätzung / Datenschutzfolgenabschätzung (DSFA)

☒Durchführung von Risikoabschätzungen inkl. Festlegung geeigneter, technisch organisatorischer Maßnahmen

☒Durchführung von Datenschutzfolgeabschätzungen

☐Ist anhand der Risikoabschätzung/ DSFA eine Verschlüsselung, Pseudonymisierung oder Anonymisierung notwendig? Zutreffendes bitte erläutern.

☐Verschlüsselung der Daten bezüglich der Verarbeitung

☐Pseudonymisierung der Daten bezüglich der Verarbeitung

☐Anonymisierung der Daten bezüglich der Verarbeitung

11 Datenschutzmanagement

Anlage 4 zum Rahmenvertrag Nr. 550001554
Annex 2 für AMP Nr. 110604 Seite A2-25

Wie ist das Datenschutzmanagmentsystem aufgestellt? z.B. Privacy by Design und Privacy by Default

Datenschutzorganisation

☒Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

☒Incident-Response-Management

☒Auftragskontrolle i.S.v. Art. 28 DSGVO

Weiteres

☐Sonstige Maßnahmen im Datenschutzmanagement:

12 Ergänzende oder erklärende Dokumente und/oder Zertifikate

Gibt es weitere Zertifikate, Sicherheitsmaßnahmen oder Kontrollprüfungsmechanismen, die Sie nachweisen können?

Zertifikate

☐ISO27001 Zertifikat, ISMS

☐Binding Corporate Rules (BCR)

☐TISAX Zertifikat

☐Sonstige Zertifikate

13 Ergänzende Maßnahmen

Bei speziellen Prozessen sind u.U. weitere Maßnahmen erforderlich - Notwendige Maßnahmen bitte ausführen.