Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO (Webshop)

1 Gegenstand und Dauer des Auftrags (Art. 28 Abs. 3 S. 1 DSGVO)

(1) Der Gegenstand des Auftrags ergibt sich aus der Zusatzvereinbarung „Webshop", auf die hier verwiesen wird (im Folgenden: Leistungsvereinbarung). Im Rahmen der Durchführung der Leistungsvereinbarung wird der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

(2) Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2 Konkretisierung des Auftragsinhalts (Art. 28 Abs. 3 S. 1 DSGVO)

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung beschrieben. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Gegenstand der Verarbeitung personenbezogener Daten sind insbesondere folgende Datenarten/-kategorien:
- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Warenkorbdaten

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen sind:
- Kunden des Auftraggebers

3 Technisch-organisatorische Maßnahmen (Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Die Dokumentation der technischen und organisatorischen Maßnahmen erfolgt in der Anlage 1.

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

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4 Berichtigung, Einschränkung und Löschung von Daten auf Weisung (Art. 28 Abs. 3 S. 2 lit. a) DSGVO)

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter

110.0676.01 P1 AUT_DE/03.2021

Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) Der Auftragnehmer ist berechtigt, der betroffenen Person Auskunft i.S.d. Art. 15 DSGVO zu erteilen.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Kapitel 4 der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt: Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Axel Moritz, privacy@payone.com bestellt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b) DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
c) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen die Daten des Auftraggebers gemäß Art. 28 Abs. 3 S. 2 lit. a), 29, 32 Abs. 4 DSGVO ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO [Einzelheiten in Anlage 1].
e) Der Auftraggeber und der Auftragnehmer arbeiten gemäß Art. 31 DSGVO auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat der Auftragnehmer ihn nach besten Kräften zu unterstützen.
h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6 Unterauftragsverhältnisse (Art. 28 Abs. 2, Abs. 3 S. 2 lit. d), Abs. 4 DSGVO)

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

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) zur Erfüllung seiner vertraglichen Leistungspflichten einsetzen. Der Auftragnehmer informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter. Der Auftraggeber ist berechtigt, Einspruch gegen die Änderung einzulegen. Im Falle eines Einspruchs ist der Auftragnehmer zur außerordentlichen Kündigung des Hauptvertrags und dieser Vereinbarung berechtigt, wenn er durch den Einspruch in der Erbringung seiner vertraglichen Leistungspflichten beeinträchtigt wird. Die Auslagerung auf Unterauftragnehmer ist nur zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2–4 DSGVO zugrunde gelegt wird.

(3) Der Auftraggeber stimmt darüber hinaus der Beauftragung der vom Auftragnehmer eingesetzten Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2–4 DSGVO. Eine Liste der eingesetzten Unterauftragnehmer des Auftragnehmers wird dem Auftraggeber auf Anfrage zur Verfügung gestellt.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

7 Kontrollrechte des Auftraggebers (Art. 28 Abs. 3 S. 2 lit. h) DSGVO)

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8 Mitteilung bei Verstößen des Auftragnehmers (Art. 28 Abs. 3 S. 2 lit. f) DSGVO)

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

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

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

9 Weisungsbefugnis des Auftraggebers (Art. 28 Abs. 3 S. 2 lit. a), Abs. 3 S. 3 DSGVO)

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

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

10 Löschung und Rückgabe von personenbezogenen Daten nach Beendigung des Auftrags (Art. 28 Abs. 3 S. 2 lit. g) DSGVO)

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

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

11 Sonstiges

(1) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrerer Regelungen werden die Vertragsparteien die unwirksame Regelung durch eine solche Regelung ersetzen, die dem ursprünglichen Zweck der unwirksamen Regelung am ehesten entspricht.

(2) Soweit andere Vereinbarungen zum Zeitpunkt des Abschlusses dieses Vertrages anderslautende oder diesem Vertrag widersprechende Angaben enthalten, so gehen die Inhalte dieses Vertrages vor.

(3) Änderungen dieser Vereinbarung bedürfen der Schriftform, das gilt auch für Änderungen des Schriftformerfordernisses.

(4) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland. Als ausschließlicher Gerichtsstand für Ansprüche, die die Parteien im Zusammenhang mit dieser Vereinbarung geltend machen, wird Frankfurt am Main vereinbart.

Anlage 1: Technisch-organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, hat die PAYONE GmbH unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken angemessene und spezifische Maßnahmen zur Wahrung der Interessen und Rechte und Freiheiten der betroffenen

Personen gemäß Artikel 32 DSGVO und § 22 BDSG vorgesehen.

Vertraulichkeit, Art. 32 Abs. 1 lit. b) DSGVO

1 Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Zutrittskontrollsystem, Ausweisleser (z.B. Magnet-/Chipkarte)
- Türsicherungen (elektrische Türöffner, Zahlenschloss etc.)
- Sicherheitstüren
- Gitter vor Fenstern/Türen in den Data Centern
- Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- Werkschutz, Pförtner
- Videoüberwachung in den Data Centern
- Biometrische Identifikation bei Zutritt zu Rechenzentren
- Spezielle Schutzvorkehrungen des Serverraums
- Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- Nicht-reversible Vernichtung von Datenträgern
- Sicherheitsbereiche/Sperrbereiche
- Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang).

2 Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- Autorisierungsprozess für Zugangsberechtigungen
- Restriktive Rechtvergabe (Need-to-know-Prinzip) mittels Rechte- und Rollenkonzept zur Begrenzung der befugten Benutzer
- Single Sign-On im Backoffice
- BIOS Passwörter
- Passwort zur Entschlüsselung von Festplatten
- Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- Personalisierte Chipkarten, Token, PIN/TAN etc. für den Remote-Zugang
- Einsatz sicherer Passwortsafes
- Protokollierung des Zugangs
- Zusätzlicher System-Log-In für bestimmte Anwendungen von privilegierten Benutzern
- Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- Firewalls

3 Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Verwaltung und Dokumentation von differenzierten Berechtigungen
- Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von personenbezogenen Daten, also der Umgang mit personenbezogenen Daten, Gegenstand der Dienstleistung ist.
- Auswertungen/Protokollierungen von Datenverarbeitungen
- Autorisierungsprozess für Berechtigungen
- Genehmigungsroutinen
- Profile/Rollen
- Verschlüsselung von CD/DVD, externen Festplatten und Laptops
- Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (Sperrung oder Verschlüsselung von Datenträgern an USB-Ports)
- „Mobile Device Management-System“
- Vier-Augen-Prinzip
- Funktionstrennung – „Segregation of Duties“
- Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- Nicht-reversible Löschung von Datenträgern
- Sichtschutzfolien für mobile Datenverarbeitungssysteme (Laptops)
- Einsatz eines SIEM-Systems

4 Trennungskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Speicherung der Datensätze in physikalisch getrennten Datenbanken
- Zugriffsberechtigungen nach funktioneller Zuständigkeit
- Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- Mandantenfähigkeit von IT-Systemen
- Verwendung von Testdaten
- Trennung von Entwicklungs- und Produktionsumgebung

5 Verschlüsselung und Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt – soweit möglich und sinnvoll – in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Die zusätzlichen Informationen werden nach Möglichkeit gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen. Es werden, sofern möglich, die personenbezogenen Daten außerhalb des Stammdatensystems durch IDs ersetzt. Dadurch wird der Datenbestand von personenbezogenen Daten auf nachfolgenden Verabeitungssystemen auf das nötige Minimum reduziert. Folgende Maßnahmen sind umgesetzt:

- Maskierung von Daten (z.B. Kreditkartennummern)
- Verschlüsselung von sensiblen Daten (z.B. Kreditkartennummern)

Integrität, Art. 32 Abs. 1 lit. b) DSGVO

6 Weitergabekontrolle

Folgende implementierte Maßnahmen stellen sicher, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder

Stellen personenbezogene Daten erhalten haben:
- Verschlüsselung von E-Mail bzw. E-Mail-Anhängen (z.B. WinZip)
- Verschlüsselung des Speichermediums von Laptops
- Gesicherter File-Transfer (z.B. sftp)
- Gesicherter Datentransport (z.B. VPN, TLS)
- Verschlüsselung von externen Festplatten oder USB-Sticks
- Verpackungs- und Versandvorschriften
- Gesichertes WLAN
- Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
- Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- Protokollierung von Datenübertragung oder Datentransport
- Protokollierung von lesenden Zugriffen (z.B. bei Kreditkartendaten)
- Nachvollziehbare Protokollierung (Kopieren, Verändern oder Entfernen von Daten)
- Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

7 Eingabekontrolle

Folgende implementierte Maßnahmen stellen sicher, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:
- Zugriffsrechte
- Systemseitige Protokollierungen
- Dokumenten-Management-System (DMS) mit Änderungshistorie
- Sicherheits-/Protokollierungssoftware
- Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- Mehraugenprinzip

Verfügbarkeit und Belastbarkeit, Art. 32 Abs. 1 lit. b) DSGVO

8 Verfügbarkeitskontrolle und Belastbarkeitskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:
- Sicherheitskonzept für Software- und IT-Anwendungen
- Back-Up-Verfahren
- Rasche Wiederherstellbarkeit
- Aufbewahrungsprozess für Back-Ups (z.B. getrennter Brandabschnitt)
- Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Spiegeln von Festplatten zwischen Rechenzentren
- Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- Geeignete Archivierungsräumlichkeiten für Papierdokumente
- Brand- und/oder Löschwasserschutz des Serverraums und der Archivierungsräumlichkeiten
- Klimatisierter Serverraum
- Virenschutz
- Firewalls
- Notfallplan
- Notfallübungen
- Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
- Redundante, örtlich getrennt betriebene IT-Systeme

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung, Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO

9 Datenschutz-Management

Folgende implementierte Maßnahmen stellen sicher, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:
- Datenschutz-Managementsystem der PAYONE GmbH
- Informationssicherheits-Managementsystem der PAYONE GmbH
- Datenschutzrichtlinie, Sicherheitsrichtlinie
- Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf die Vertraulichkeit
- Regelmäßige Schulungen der Mitarbeiter zum Datenschutz und zur Informationssicherheit
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung von Datenschutz-Folgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
- Externe Prüfung/Auditierung des Datenschutzes und der Informationssicherheit (z.B. Datenschutzaudit, PCI-DSS, KRITIS)

10 Incident-Response-Management

Folgende implementierte Maßnahmen stellen sicher, dass im Falle von Datenschutzverstößen Meldeprozesse ausgelöst werden:
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

11 Datenschutzfreundliche Voreinstellungen

Gemäß Art. 25 Abs. 2 DSGVO sind die Default-Einstellungen sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z.B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z.B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z.B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt:
- Beachtung des Datenschutzgrundsatzes zur Datenvermeidung
- Beachtung des Datenschutzgrundsatzes zur Datensparsamkeit

– Zugriffsberechtigungen, die sich am Business-Need orientieren
– Einschränkung von Daten-Exporten
– Passwortwechsel beim ersten Login
– Beachtung der Speicherfristen von Daten

12 Auftragskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

– Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
– Prozess zur Erteilung und/oder Befolgung von Weisungen
– Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
– Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
– Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
– Prüf- und Kontrollrechte des datenschutzrechtlich Verantwortlichen einer Datenverarbeitung
– Unabhängige Auditierung der Weisungsgebundenheit
– Verpflichtung der Mitarbeiter auf die Verschwiegenheit
– Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
– Formalisiertes Auftragsmanagement
– Dokumentiertes Verfahren zur Auswahl des Dienstleisters
– Standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister

Stand: Januar 2021