Datenschutzkonzept

Zweck & Header

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen und kann auch als Grundlage für datenschutzrechtliche Prüfungen z.B. durch Auftraggeber im Rahmen der Auftragsdatenverarbeitung genutzt werden.

Attribute	Werte
Dokumententyp	Richtlinie
Klassifikation	Intern
Document Owner	Datenschutzbeauftragter der PlusServer GmbH
Document Manager	Director IT-Security & Processes
Version	1.2 DE
In Kraft seit	11.09.2018
Betrifft	Mitarbeiter / Kunden / Interessenten der PlusServer GmbH
Sichtbar für	Mitarbeiter der PlusServer

Änderungshistorie

Version	Datum	Änderungen
1.0 DE	21.06.2017	Erstveröffentlichung
1.1 DE	10.11.2017	Anpassungen der Geschäftsführung in der Fußzeile
1.2 DE	11.09.2018	Anpassungen an die Anforderungen der Datenschutzgrundverordnung (DSGVO)

PlusServer GmbH
Hohenzollernring 72
50672 Köln
Deutschland

Kontakt
Beratung: +49 2203 - 1045 3500
Support: +49 2203 - 1045 3600
Buchhaltung: +49 2203 - 1045 3700
E-Mail: info@plusserver.com

Sitz
Amtsgericht Köln,
HRB 84977

Umsatzsteuer-ID
DE815289260

Geschäftsführung
Thomas Noglik (CEO)
Holger Müller
Daniel Thomy
Bernd Vogtland

Inhaltsverzeichnis

1. Sicherheitspolitik

Die PlusServer GmbH betreibt ein Informationssicherheitsmanagementsystem (ISMS) das neben der Informationssicherheit auch die Aspekte des Datenschutzes nach der Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) abdeckt. Neben den klassischen Zielen der Vertraulichkeit, Integrität und Verfügbarkeit von Daten, umfasst die Zielsetzung auch die Einhaltung von gesetzlichen Regelungen, insbesondere denen der DSGVO und des BDSG.

2. Verantwortlichkeiten im Unternehmen

Die Verantwortlichkeiten sind in der Sicherheitsleitlinie des Unternehmens und in der Rollen- und Aufgabenbeschreibung definiert. Des Weiteren sind die Verantwortlichkeiten im Bereich Datenschutz im öffentlichen Verfahrensverzeichnis einsehbar.

3. Rechtliche Rahmenbedingungen

Aufgabe des Datenschutzes ist es nach Art. 1 Datenschutzgrundverordnung (DSGVO) den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und die Verwendung seiner Daten zu bestimmen („informationelles Selbstbestimmungsrecht“). Das gesamte Datenschutzrecht bezieht sich nur auf personenbezogene Daten. Darunter sind „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ zu verstehen. Juristische Personen werden nicht erfasst.

Die Datenschutzgrundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, trat am 28.05.2018 und hat zum Ziel das Datenschutzrecht europaweit zu harmonisieren. Die Verordnung ersetzt die Richtlinie 95/46/EG und gilt anders als noch die Richtlinie unmittelbar ohne Umsetzungsakt in allen Ländern.
Auf Grund verschiedener Konkretisierung- und Öffnungsklauseln in der DSGVO gelten neben der Verordnung die Regeln des Bundesdatenschutzgesetzes (BDSG), dass ebenfalls am 28.05.2018 in Kraft trat.
Neben dem BDSG wird das Datenschutzrecht noch durch die Datenschutzgesetze der Länder und eine Vielzahl anderer bereichsspezifischer Vorschriften, wie dem TKG, TMG und dem BetrVG, rechtlich ausgestaltet.

Grundsätzliche Prinzipien des Datenschutzrechts, wie das sog. Verbot mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datenvermeidung/-sparsamkeit sind auch nach Inkrafttreten der DSGVO maßgeblich.

Die PlusServer GmbH versichert, dass sie alle Sie betreffenden datenschutzrechtlichen Vorschriften beachtet und einhält, um so ein Hohes Maß an Sicherheit bei der Verarbeitung personenbezogener Daten zu gewährleisten.

4. Schutzbedarf der Daten

Der Schutzbedarf der Kundenstammdaten wurde mit „hoch“ für die Kategorien Vertraulichkeit, Integrität und Verfügbarkeit bewertet und die entsprechenden Maßnahmen dieser Bewertung angepasst bzw. umgesetzt. Eine Bewertung des Schutzbedarfs der Daten, welche auf den von uns angebotenen Produkten und Services durch den Kunden verarbeitet werden, kann nicht einheitlich definiert werden. Grundsätzlich streben wir ein Sicherheitsniveau für einen Schutzbedarf von „hoch“ bis „sehr hoch“ an. Letztlich entscheidet der Kunde mit der Wahl der Produkte, dem abgeschlossenen Service-Vertrag und den vereinbarten SLAs, über das zu erreichende Sicherheitsniveau seines Servers bzw. seiner Hosting-Umgebung.

5. Interne und Externe Überprüfungen

Mittels national und international anerkannten Zertifikaten, z.B. ISO 27001 (nativ), PCI DSS und ISO 27001 auf Basis von IT Grundschutz, weisen wir unseren Kunden transparent das Sicherheitsniveau unseres Unternehmens nach. Im Rahmen der Zertifizierungen werden unsere Sicherheitsmaßnahmen mindestens viermal pro Jahr durch externe Fachleute überprüft.

Teil des durch die PlusServer GmbH betriebenen ISMS ist eine jährliche Wirksamkeitskontrolle die intern die Umsetzung von risikominimierenden Maßnahmen und die Umsetzung der definierten Richtlinien und Prozesse kontrolliert.

6. Technische und organisatorische Maßnahmen

Gemäß Art. 32 Datenschutzgrundverordnung (DSGVO) sind alle Stellen, welche personenbezogene Daten verarbeiten, erheben oder nutzen verpflichtet, technische und organisatorische Maßnahmen zu treffen um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen der DSGVO erfüllt sind.

Die technischen und organisatorischen Maßnahmen der PlusServer GmbH sind im Anhang einsehbar. Sie sind Teil der Vereinbarungen zur Auftragsdatenverarbeitung die wir mit unseren Kunden abschließen.

7. Organisatorische Mindestregelungen

Verantwortliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, haben die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Ein wesentlicher Bestandteil stellt dabei die Einbeziehung der Mitarbeiter des jeweiligen Unternehmens dar. Gerade diese Personengruppe ist als wichtiger Adressat der Vorgaben zum Datenschutz anzusehen, da ihre Tätigkeit in einer digitalisierten Arbeitswelt einen fortwährenden Umgang mit personenbezogenen Daten bedingt.
Das Gestaltungsmittel von Unternehmensrichtlinien und -konzepten ist dabei eine Möglichkeit, bestehende Vorgaben zum Datenschutz in zentralen Dokumenten zu verankern und die Adressaten mit den datenschutzrechtlichen Vorgaben vertraut zu machen.

Die PlusServer GmbH hat von dieser Gestaltungsmöglichkeit Gebrauch gemacht und verschiedene Unternehmensrichtlinien und -konzepte erarbeitet, um so verbindliche Regeln für alle Betriebsteile aufzustellen, die die Sicherheit von personenbezogenen Daten im Unternehmen stärkt und den betrieblichen Ansatz eines allumfassenden Datenschutzes unterstreicht. Da die im

Folgenden dargestellten Regelungen verbindlichen Charakter haben, können Verstöße gegen die Inhalte der Richtlinien zu arbeitsrechtlichen Konsequenzen führen.

IT-Nutzungsrichtlinie

Die IT-Nutzungsrichtlinie der PlusServer GmbH umfasst Vorgaben zur Organisation, zur Administration und zur Nutzung von E-Mail- und Internetdiensten. Die Richtlinie enthält ferner Vorgaben zum datenschutzkonformen Umgang mit Mobile Devices und Wechselmedien.

Datensicherungskonzept

Der Verlust von Daten kann erhebliche Auswirkungen auf die Geschäftsfähigkeit haben. Darüber hinaus existieren gesetzlich verpflichtende Regelungen, die einzuhalten sind.

Das Datensicherungskonzept der PlusServer GmbH soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

Virenschutzkonzept

Ziel des Virenschutzkonzepts der PlusServer GmbH ist die Unterstützung der Schaffung eines effektiven Computer-Viren-Schutzes für die IT-Systeme sowie die Dokumentation aller diesbezüglichen Entscheidungen.

Notfallvorsorgekonzept

Das Notfallvorsorgekonzept der PlusServer GmbH hat zum Ziel, die Geschäftstätigkeit während eines Ausfalls eines IT-Systems oder einer IT-Anwendung aufrechtzuerhalten und sicherzustellen sowie die Betriebsfähigkeit innerhalb einer tolerierbaren Zeitspanne wiederherzustellen. Das Notfallvorsorgekonzept beschreibt hierzu, welche Maßnahmen zur Vorbereitung auf Notfälle unternommen werden und was im Notfall zu tun ist.

Berechtigungskonzept

Im Berechtigungskonzept der PlusServer GmbH werden Zugriffsregeln für Benutzergruppen, in Ausnahmefällen auch einzelner Benutzer, auf Daten eines IT-Systems festgelegt. Außerdem werden dort alle Prozesse, die die Umsetzung des Berechtigungskonzepts betreffen beschrieben, wie z.B. das Löschen und Erstellen von Nutzern, oder Passwortrestriktionen.

Dies führt dazu, dass Mitarbeiter nur soweit auf Systeme und Daten Zugriff erhalten, wie es für ihre Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“).

Konzept zur Protokollierung

Das Konzept zur Protokollierung der PlusServer GmbH hat zum Ziel, wesentliche Veränderungen an IT-Systemen, Netzen oder Anwendungen nachvollziehen zu können, um deren Sicherheit aufrechterhalten zu können.

8. Datenschutzrechtliche Anforderungen

Bestellung und Aufgaben des Datenschutzbeauftragten

Ein Datenschutzbeauftragter wirkt in einer Organisation auf die Einhaltung des Datenschutzes hin. Er muss die notwendige Fachkunde für die Ausübung besitzen und darf nicht in einen Konflikt oder in die Gefahr der Selbstkontrolle geraten. Die Aufgabe und Tätigkeit eines Datenschutzbeauftragten wird in den Art. 37 ff. DSGVO geregelt.
Als Externer Datenschutzbeauftragter ist für die PlusServer GmbH bestellt:

KINAST Rechtsanwaltsgesellschaft mbH
Hohenzollernring 54
50672 Köln
info@plusserver.com

Verzeichnis aller Verfahren und der verarbeiteten personenbezogenen Daten.

Ein internes Verfahrensverzeichnis wird in Zusammenarbeit mit dem Datenschutzbeauftragten gepflegt. Dieses umfasst alle Verfahren in denen personenbezogene Daten verarbeitet werden.

Datenschutz-Folgenabschätzung

Nach Art. 35 DSGVO unterliegt die Datenverarbeitung der „Datenschutz-Folgenabschätzung“, wenn sie besondere Risiken für die Rechte und Freiheiten des Betroffenen aufweist. Dies ist insbesondere dann gegeben, wenn besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet werden
oder die Verarbeitung der Daten der Bewertung der Persönlichkeit des Betroffenen dienen soll einschließlich seiner Fähigkeiten, seiner Leistung und seines Verhaltens. Die Datenschutz-Folgenabschätzung wird nach Art. 35 Abs. 2 DSGVO durch den Datenschutzbeauftragten durchgeführt, sofern ein solcher benannt wurde..
Jede Datenverarbeitung wird bei der PlusServer GmbH durch den Externen Datenschutzbeauftragten geprüft und, wenn nötig, im Rahmen einer Datenschutz-Folgenabschätzung auf Ihre datenschutzrechtliche Zulässigkeit kontrolliert.

Datenschutz-Schulung und Verpflichtung der Mitarbeiter auf das Datengeheimnis

Alle Mitarbeiter werden bei Einstellung auf die datenschutzrechtliche Vertraulichkeit und § 88 TKG verpflichtet. Darüber hinaus finden jährlich Schulungen zum Thema Datenschutz statt. Zusätzliche Awarenessmaßnahmen wie Poster, oder E-Mails zu aktuellen Datenschutz-relevanten Themen, sorgen für ein stetes Bewusstsein für dieses wichtige Thema.

Vertragliche Regelungen der Auftragsverarbeitung

Auftragsverarbeitung im Sinne der DSGVO ist die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Dienstleister im Auftrag der verantwortlichen Stelle. Art. 28 DSGVO beschreibt welche Rechte, Pflichten und Maßnahmen im Einzelnen durch den Vertrag zwischen Auftraggeber (verantwortliche Stelle) und Auftragnehmer (Dienstleister) zu treffen sind.

Die PlusServer GmbH versichert, jede Auftragsverarbeitung durch Abschluss einer entsprechenden, schriftlichen Vereinbarung zur Auftragsverarbeitung legitimiert zu haben.