Technische und organisatorische Maßnahmen

v1.4 vom 04.07.2018

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen der

Ambrosia FM Consulting & Services GmbH

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

1.1 Zutrittskontrolle

Die Zentrale der Ambrosia FM Consulting & Services GmbH (im Folgenden ‚ambrosia' genannt) ist mittels eines elektronischen Zutrittskontrollsystems gesichert. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Besuchern ist der Zutritt zu Räumen der ambrosia nur mit Besucherausweis und in Begleitung eines Mitarbeiters der ambrosia gestattet. Die ambrosia verfügt über zwei Standorte an denen folgende Maßnahmen getroffen wurden:

Standort Bad Oeynhausen (Zentrale)

- Das Gebäude ist über Zäune und Pforten gesichert.
- Der Empfangsbereich des Gebäudes ist während der Öffnungszeiten Mo. – Do. von 08:00 bis 17:00 Uhr und am Fr. von 08:00 bis 14:00 durch eine Empfangsdame besetzt. Es findet eine Besucherprotokollierung statt.
- Videoüberwachung der Ein- und Ausgangsbereiche.
- Schließsystem mit personalisierten LEGIC-Zutrittskarten. Öffnungszeiten von Türen und Toren werden elektronisch protokolliert.
- Der Räumlichkeiten in Bad Oeynhausen sind von der Balda Medical GmbH & Co. KG angemietet. Die Vermieterin stellt die Sicherheit der oben Beschriebenen Maßnahmen sicher.
- Die Serverräume dürfen nur zu zweit betreten werden.

Standort Berlin

- Gebäudesicherung über Zylinderschließanlage.
- Am Standort Berlin befinden sich keine Serversysteme der ambrosia.

Home-Office Arbeitsplätze unterliegen einer Home-Office Regelung welche den Zugriff auf die Ambrosia-Netze und den Umgang mit Aktenordnern und Dokumenten regelt. Dabei findet der IT-Zugriff auf ambrosia Systeme ausschließlich über eine VPN-Verbindung statt. Dokumente und Akten sind immer verschlossen aufzubewahren.

1.2 Zugangskontrolle

Der Zugang zu Datenstationen (PC, Server, Netzwerkkomponenten) erfolgt durch Berechtigungsvergabe und Authentifizierung in allen Systemen. Die Zugangsregelungen umfassen folgende Maßnahmen:

- Passwort-Richtlinie welche per Gruppenrichtlinie gesteuert wird und Mindestlänge und regelmäßigen Wechsel vorschreibt. Kennwörter können nicht mehrfach verwendet werden.
- Alle Systeme sind durch Einsatz einer Hardware-Firewall gesichert welche kontinuierlich auf einem aktuellen Patch- und Updatelevel gehalten wird.
- Einsatz einer MDM-Lösung zur Fernadministration mobiler Endgeräte (z.B. Sperren und löschen von Daten). Private Geräte sind grundsätzlich nicht für berufliche Nutzung zugelassen. Private Geräte haben keinen Zugriff auf das Firmennetzwerk. Es steht ein Gast-Zugang zur Verfügung welcher strikt vom Firmennetzwerk getrennt ist.
- Die Systeme der ambrosia sind durch Antispyware / Antivirensoftware gesichert welche laufend aktualisiert werden.
- Mobile Endgeräte werden mindestens auf Basis von Android 6.0 oder iOS 10 eingesetzt und über ein MDM zentral aktualisiert.
- Es werden Windows 7 und Windows 10 Desktopbetriebssysteme eingesetzt welche durch ein zentrales Patch- und Updatemanagement auf einem aktuellen Stand gehalten werden.
- Zeitgesteuerte Bildschirmsperren mit Kennwortreaktivierung per GPO erzwungen.

1.3 Zugriffskontrolle

- Die Daten auf den ambrosia-Systemen sind durch ein Rechte- / Rollen- Konzept gegen unbefugten Zugriff und vor Veränderung / Löschung geschützt.
- Es gibt ein Backupkonzept, sodass bei Veränderung / Löschung auf vorherige Datenstände zurückgegriffen werden kann. (siehe Punkt 3)
- Innerhalb der ambrosia werden die Zugriffsmöglichkeiten auf das ‚Need to Know' Prinzip beschränkt. Sollte ein unberechtigter Zugriff dennoch möglich sein, erfolgt eine Eskalation an die IT – Abteilung und das Rechte-/Rollen Konzept wird umgehend angepasst.

1.4 Trennungskontrolle

- Zur Sicherstellung des Produktivbetriebs sind alle Produktivsysteme von Entwicklungs- und Testsystemen vollständig getrennt.
- Ein Zugriff auf die Systeme erfolgt ausschließlich durch Berechtigte.
- Die Testsysteme sind auch physikalisch von Produktivsystemen getrennt.

1.5 Pseudonymisierung

Die von uns eingesetzten Systeme und Verfahren unterstützen auf verschiedene Art und Weise die Pseudonymisierung von personenbezogenen Daten. In Abstimmung mit dem Kunden und mit Bezug auf das Konkrete Projekt erfolgt bei Bedarf eine bilaterale Vereinbarung zur Pseudonymisierung von personenbezogenen Daten, welche wir im Rahmen unserer Tätigkeit verarbeiten. Dies sind immer Einzel-Projektbezogen und werden systemisch und durch Organisationsanweisungen im Unternehmen umgesetzt. Je nach vereinbarten Anforderungen an ein Lösch- und Pseudonymisierungskonzept kommen dabei in der Regel dann ein zentrales System zur Verwaltung der personenbezogenen Daten zum Einsatz. In Folgesystemen sowie innerhalb des Datenbestandes des führenden Systems werden je identifizierbarer Person direkt Pseudonyme vergeben und die Verbindung zur konkreten Person nur im führenden System hergestellt.

Eine Pseudonymisierung der verwalteten und gespeicherten Datenbestände erfolgt sodann durch Entfernen der identifizierbaren personenbezogenen Angaben im führenden System bzw. durch Löschen der gesamten Tabelle. Dabei wird per Organisations-Regeln darauf geachtet, dass der Datenbestand, für den eine Pseudonymisierung vorgesehen wird, ausreichend groß ist um sicherzustellen, dass ohne das führende System nicht durch Rückschlüsse auf einzelne identifizierbare Personen noch möglich sind. Gleichzeitig wird per Organisationsregel sichergestellt, dass der Datenbestand erst dann als hinreichend pseudonymisiert gilt, wenn auch ausreichend Personen als nicht mehr identifizierbar gelten so dass nicht alleine aus der Tatsache, dass eine Person nicht mehr identifizierbar ist, schon die Schlussfolgerung auf die konkrete Einzelperson gelingt.

Wo es möglich ist, werden im Anschluss nur noch die durch das führende System vergebenen Pseudonyme in weiterverarbeitenden Systemen zur Zuordnung von Informationen zu Individuen eingesetzt.

1.6 Maßnahmen zur Verschlüsselung der Daten

Bei der ambrosia werden anlassbezogen folgende Verschlüsselungstechniken eingesetzt:

- TLS-Verschlüsselung im Emailverkehr
- Teilweise Festplattenverschlüsselung
- Teilweise Verschlüsselung der Datenbank und Datenträger von Backupsystemen
- Einsatz VPN
- Teilweise Verschlüsselung von Notebooks und mobilen Datenträgern

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

2.1 Weitergabekontrolle

Die Datenübertragung zwischen Servern und Arbeitsplätzen der ambrosia erfolgt bei Nutzung von internetbasierten Anbindungen in Form einer verschlüsselten VPN Anbindung. Die Übermittlung von Daten an Dritte – Steuer- und Meldebehörden – erfolgt mit den von den staatlichen Stellen vorgegebenen Kommunikationswegen.

Weitere Maßnahmen:

- Regelung zum Umgang mit mobilen Datenträgern.
- Datenübergaben werden über eine eigens betriebene private Cloud über Https und ein dediziertes Kennwort abgewickelt. Die Cloud-Lösung wird bei der Fa. Mittwald CM Service GmbH & Co. KG in Espelkamp gehostet.
- Ausschussmaterial, Testausdrucke sowie defekte Speichermedien werden ausschließlich durch ein zertifiziertes Entsorgungsunternehmen DSGVO-Konform vernichtet. Mitarbeiter sind dazu verpflichtet personenbezogene Daten über die DSGVO-Tonne zu vernichten.
- Festlegung von Empfängerkreisen.
- organisatorische Festlegung zum Zugriff auf Kundensysteme durch Mitarbeiter der ambrosia welche den Standards der DSGVO und darüber hinaus entsprechen. Darüber gewährleisten wir die Einhaltung von allen mit Kunden geschlossenen AVVs.

2.2 Eingabekontrolle

- Die eingesetzten Softwaresysteme unterziehen die Eingaben in Formularfeldern einer Plausibilitätsprüfung.
- Alle Benutzer und Arbeitsstationen können im Netzwerk eindeutig identifiziert werden.
- Änderungen in Softwaresystemen werden auf den Servern protokolliert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DS-GVO)

Es findet eine Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust) statt. Dies umfasst die folgenden Maßnahmen:

- Die Serversysteme sind durch eine Unterbrechungsfreie Stromversorgung und Überspannungsschutz gegen Ausfall gesichert.
- Schutz vor Diebstahl durch Zutrittskontrolle in die Serverräume. Die Serverschränke sind durch ein Schloss vor unbefugter Öffnung gesichert. Zutritt zu Serverräumen nur in Begleitung.
- Alle Systeme sind durch und Virenschutz / Firewall abgesichert.

- Im gesamten Gebäude existiert eine Brandmeldeanlage.
- Die Server sind in klimatisierten Serverräumen in 19“ Racks untergebracht.
- Die Daten liegen redundant auf RAID-6 Speicher.
- Die Server werden täglich auf einen räumlich getrennten Backupserver in einem gesonderten Brandabschnitt gesichert.
- Weiterhin sieht das Backupkonzept eine wöchentliche Vollsicherung vor mit täglichen inkrementellen Backups. Vollbackups werden über einen längeren Zeitraum aufgehoben.
- Eine Offline Kopie der wöchentlichen Voll-Backups wird erstellt und geografisch getrennt aufbewahrt.
- Die Funktionsfähigkeit der Backups wird regelmäßig geprüft.
- Die Systemverfügbarkeit und Performance wird kontinuierlich mit einem Infrastruktur-Monitoring Werkzeug überprüft.

Diese definierten Standards gelten für alle Serversysteme, die von der ambrosia betrieben werden.

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

4.1 Datenschutz-Management

Alle Mitarbeiter sind auf das Datengeheimnis und die Einhaltung von Betriebs- und Geschäftsgeheimnissen verpflichtet worden und sind gemäß Artikel 32 und Artikel 29 DSGVO angewiesen, personenbezogene Daten nur auf Anweisung des Verantwortlichen zu verarbeiten.
Über eine EDV-Organisationsanweisung ist der Umgang mit Firmeneigenen Datenverarbeitungsanlagen (Server und Notebooks) geregelt. Dies umfasst insbesondere auch den Einsatz von Firmenhardware außerhalb des Betriebsgeländes. Es sind Datenschutz-Koordinatoren benannt welche als Ansprechpartner für Datenschutzfragen fungieren.

4.2 Security- und Risikomanagement

Die ambrosia wickelt ihre Leistungen auf der Grundlage eines gelebten Informationssicherheitsmanagements ab. Die eingesetzten Sicherheitsverfahren werden laufend überprüft.

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

Durch datenschutzfreundliche Voreinstellungen (“Privacy by Design and by Default”) der von uns eingesetzten Systeme werden unrechtmäßige Erhebung, Verarbeitung oder Missbrauch von Daten präventiv verhindert. Über angemessene technische Voreinstellungen soll sichergestellt werden, dass grundsätzlich nur die personenbezogenen Daten erhoben und verarbeitet werden, die für den konkreten Zweck auch tatsächlich erforderlich sind.

Um eine risikoarme Verarbeitung personenbezogener Daten zu erreichen, werden u. a. folgende Schutzmaßnahmen umgesetzt:

- Menge der personenbezogenen Daten minimiert.
- Daten so früh wie und wo möglich pseudonymisiert oder verschlüsselt.
- Transparenz in Bezug auf die Funktionen und die Verarbeitung der Daten hergestellt.
- Daten so früh wie möglich gelöscht oder anonymisiert.
- Zugriffsmöglichkeiten auf Daten minimiert.
- Vorhandene Konfigurationsmöglichkeiten auf datenschutzfreundlichste Werte voreingestellt.

4.4 Auftragskontrolle

Es findet keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne vertragliche Grundlage (AVV) und ohne entsprechende Weisung des Auftraggebers statt. Dies umfasst unter anderem:

- Eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement
- Vorabüberzeugungspflicht
- Gelebtes Vertragsmanagement
- Qualitätsmanagement und -system

4.5 Verzeichnis von Verarbeitungstätigkeiten:

Entsprechend DSGVO existiert ein Verzeichnis von Verarbeitungstätigkeiten. Dieses umfasst alle Systeme, Tools und Prozesse im Unternehmen, in welchen personenbezogenen Daten verarbeitet werden. Das Verzeichnis von Verarbeitungstätigkeiten wird kontinuierlich fortgeschrieben und aktualisiert.

4.6 Vertragsmanagement:

Es gibt ein Vertragsmanagement (siehe oben). Die Prozesse im Vertragsmanagement wurden im Zuge der DSGVO-Einführung überprüft und erweitert. Dies umfasst:

- Die vertragsbezogene Prüfung, ob im Rahmen des Vertragsverhältnisses personenbezogene Daten erhoben, genutzt, übermittelt oder verarbeitet werden
- ob eine Vereinbarung zur Auftragsdatenverarbeitung nach Art. 28 DSGVO erforderlich ist und
    - ob diese bereits abgeschlossen wurde
    - oder geschlossen werden muss
- Die Prüfung der Inhalte des AV-Vertrages entsprechend eigener Qualitätsstandards

Technische und organisatorische Maßnahmen

v1.4 vom 04.07.2018

Zu beachten:

Wir unterziehen unsere eigenen Maßnahmen einer jährlichen Selbstauditierung.
Dieses Dokument ist immer in der aktuellen Version unter folgender URL abrufbar:

https://ambrosia-fm.de/dsgvo/ambrosia-toms.pdf