PLANIT// PRIMA

Export vom 29.11.2023

konfidal GmbH
Beschreibung nach Art. 30 Abs. 1 DSGVO

Datenschutzdokumente für die Filzfabrik Wurzen GmbH

Allgemeine Angaben	
1.1	**Name und Kontaktdaten des Verantwortlichen** -
1.2	**EU-Vertreter des Verantwortlichen** -
1.3	**Vertreter des Verantwortlichen**
1.4	**Datenschutzbeauftragter des Verantwortlichen**
1.5	**Mit der Leitung der Datenverarbeitung betraute Personen**

Angaben zum Verfahren	
2.1	**Fachverantwortlicher** -
2.2	**IT-Verantwortlicher für dieses Verfahren** -
2.3	**Zweck der Verarbeitung**
2.3.1	**Beschreibung der Datenverarbeitung** Webbasierte Software in die Hinweisgeber Informationen über Rechtsverstöße eingeben können um diese an den Verantwortlichen zu melden.

2.3.2	**Zweck** ☐ Durchführung von Beschäftigungsverhältnissen ☐ Erfüllung von vertraglichen Pflichten gegenüber den Betroffenen ☐ Erfüllung anderer vertraglicher Pflichten ■ Verfolgung berechtigter Interessen ■ andere Zwecke: Erfüllung von Pflichten nach dem Hinweisgeberschutzgesetz
2.4	**Betroffene Personengruppen** ■ Beschäftigte ■ Lieferanten ■ Dienstleister ■ Kunden
2.5	**Kategorien personenbezogener Daten**
2.5.1	**Persönliche Angaben, insbesondere** ■ Name ■ E-Mail
2.5.2	**Vertragsdaten, insbesondere über** -
2.5.3	**Beschäftigtendaten, insbesondere Angaben über** -
2.5.4	**Telekommunikations-, Telemediendaten und ähnliche Daten** ■ IP-Adressen
2.5.5	**Besondere Kategorien personenbezogener Daten, nämlich Angaben über** -
2.5.6	**Zahlungsdaten** -
2.5.7	**Aufnahmen, nämlich insbesondere** -
2.5.8	**Andere** Inhalte der Meldung

2.6	**Kategorien von Empfängern, denen die Daten offengelegt wurden oder werden** ■ Beschäftigte
2.7	**Übermittlung in Drittländer (außerhalb des europäischen Wirtschaftsraums/ EWR) oder in eine internationale Organisation** ◉ keine
2.8	**Bei Übermittlungen in Drittländer: Rechtsgrundlage** -
2.9	**Regelfristen für die Löschung**
2.9.1	**Sperrfrist** -
2.9.2	**Löschfrist** 3 Jahre nach Eingang der Meldung
2.9.3	**Wenn ein Löschkonzept vorliegt, hier hochladen oder verlinken** -

technisch-organisatorische Maßnahmen

3.1	**Eingesetzte Datenverarbeitungsanlagen** ■ ausgelagerte Server ■ eigene Server ■ Desktop Clients ■ Mobile Clients
3.2	**Eingesetzte Software und Dienstleister** konfindal Hinweisgebersystem
3.3	**Zugriffsberechtigte Personen (Abteilung/Rolle)** -
3.4	**Allgemeines Sicherheitskonzept** -
3.5	**Besondere Sicherheitsmaßnahmen für diesen Prozess**

3.5.1	**Zutrittskontrolle** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.2	**Zugangskontrolle** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.3	**Zugriffskontrolle** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.4	**Weitergabekontrolle** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.5	**Eingabekontrolle** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.6	**Auftragskontrolle** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.7	**Verfügbarkeitskontrolle** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.8	**Trennungskontrolle** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.9	**Pseudonymisierung und Verschlüsselung** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.10	**Belastbarkeit / Resilienz** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.11	**Rasche Wiederherstellung** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters

3.5.12	**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit technisch-organisatorischer Maßnahmen** ■ siehe Konzept zum technisch-organisatorischen Datenschutz des Auftragsverarbeiters
3.5.13	**Wenn ein eigenes TOM-Konzept existiert, hier verlinken oder hochladen** -
3.5.14	**Wenn TOM-Konzepte von Auftragsverarbeitern existieren, hier verlinken oder hochladen** -

Weitere Angaben

4.1	**Herkunft der Daten** ■ Direkterhebung beim Betroffenen ■ Erhebung bei Dritten, nämlich: Hinweisgebern
4.2	**Rechtsgrundlagen**
	■ Erfüllung einer rechtlichen Verpflichtung ■ Wahrung berechtigter Interessen
	Einschlägige Norm(en): Art. 6 Abs. 1 lit. c und f

Datenschutz-Folgenabschätzung

5.1	**Risiko für die Rechte und Freiheiten natürlicher Personen** -
5.2	**Bei hohem Risiko: Datenschutz-Folgenabschätzung** ◉ durchgeführt am
5.3	**Wenn Datenschutz-Folgenabschätzung durchgeführt wurde: Hier hochladen oder verlinken** -

5.4	**Wenn Vorprüfung zur Datenschutz-Folgenabschätzung (Schwellwertprüfung) durchgeführt wurde: Hier hochladen oder verlinken** -

PLANIT// PRIMA

Export vom 29.11.2023

konfidal GmbH
Standardvertragsklauseln (AVV/DPA innerhalb EU/EWR)

Datenschutzdokumente für die Filzfabrik Wurzen GmbH

STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

(a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

(b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

(c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

(d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

(e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

(f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

(a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

(b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

(a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

(b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

(c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

Kopplungsklausel

(a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

(b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

(c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II - PFLICHTEN DER PARTEIEN

Klausel 1

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 2

Pflichten der Parteien

2.1 Weisungen

(a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

(b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

2.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

2.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

2.4 Sicherheit der Verarbeitung

(a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

(b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

2.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

2.6 Dokumentation und Einhaltung der Klauseln

(a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

(b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

(c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

(d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

(e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

2.7 Einsatz von Unterauftragsverarbeitern

(a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens zwei Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

(c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

(d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

(e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

2.8 Internationale Datenübermittlungen

(a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

(b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 3

Unterstützung des Verantwortlichen

(a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

(b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

(c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

  (i) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

  (ii) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

  (iii) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

  (iv) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

(d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 4

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

4.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

(a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

(b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

  (i) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

  (ii) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

  (iii) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

(c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

4.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

(a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

(b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

(c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III - SCHLUSSBESTIMMUNGEN

Klausel 1

Verstöße gegen die Klauseln und Beendigung des Vertrags

(a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/ oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

(b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn:

(i) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

(ii) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

(iii) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

(c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

(d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I - LISTE DER PARTEIEN

Verantwortliche(r)

Name	-
Anschrift	-
Name, Funktion und Kontaktdaten der Kontaktperson	-
Unterschrift und Beitrittsdatum	-

Auftragsverarbeiter

Name	konfidal GmbH
Anschrift	Hauptstraße 28, 15806 Zossen
Name, Funktion und Kontaktdaten der Kontaktperson	Martin Meng
Unterschrift und Beitrittsdatum	-

ANHANG II - BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen,

deren personenbezogene Daten verarbeitet werden	Beschäftigte, Kunden, Lieferanten, Dritte die in Meldungen benannt werden
Kategorien personenbezogener Daten, die verarbeitet werden	Kontaktdaten und Inhhalte von Meldungen
Verarbeitete sensible Daten (falls zutreffend)	möglich als Inhalt von Meldungen
Art der Verarbeitung	Erhebung und Weiterleitung von Meldungen
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden	Erhebung und Weiterleitung von Meldungen
Dauer der Verarbeitung	Nach Kundenspezifikation
Verarbeitung durch (Unter-)Auftragsverarbeiter	Hosting durch Hetzner Online GmbH

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Hat der Auftragsverarbeiter ein Konzept für den technisch-organisatorischen Datenschutz (TOM-Konzept) vorgelegt?

◉ Ja

Das TOM-Konzept des Auftragsverarbeiters hier hochladen oder verlinken

hetzner-TOM.pdf

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt

Unterauftragsverarbeiter

Name	Hetzner Online GmbH
Anschrift	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland
Name, Funktion und Kontaktdaten der Kontaktperson	-
Beschreibung der Verarbeitung	Hosting

EU Standardvertragsklauseln (Auftragsdatenverarbeitung innerhalb des EWR)

	■ Kopplungsklausel einfügen
Unterauftragsverarbeiter	
	◉ Allgemeine, schriftliche Genehmigung für Unterauftragsverarbeiter
	zwei Wochen

ANHANG I - LISTE DER PARTEIEN

Verantwortliche(r)	
Name	-
Anschrift	-
Name, Funktion und Kontaktdaten der Kontaktperson	-
Unterschrift und Beitrittsdatum	-
Auftragsverarbeiter	
Name	konfidal GmbH
Anschrift	Hauptstraße 28, 15806 Zossen
Name, Funktion und Kontaktdaten der Kontaktperson	Martin Meng
Unterschrift und Beitrittsdatum	-

ANHANG II - BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden	Beschäftigte, Kunden, Lieferanten, Dritte die in Meldungen benannt werden

Daten, die verarbeitet werden	

Kategorien personenbezogener Daten, die verarbeitet werden	Kontaktdaten und Inhhalte von Meldungen
Verarbeitete sensible Daten (falls zutreffend)	möglich als Inhalt von Meldungen
Art der Verarbeitung	Erhebung und Weiterleitung von Meldungen
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden	Erhebung und Weiterleitung von Meldungen
Dauer der Verarbeitung	Nach Kundenspezifikation
Verarbeitung durch (Unter-)Auftragsverarbeiter	Hosting durch Hetzner Online GmbH

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Hat der Auftragsverarbeiter ein Konzept für den technisch-organisatorischen Datenschutz (TOM-Konzept) vorgelegt?

◉ Ja

Das TOM-Konzept des Auftragsverarbeiters hier hochladen oder verlinken

hetzner-TOM.pdf

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt

Unterauftragsverarbeiter

Name	Hetzner Online GmbH
Anschrift	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland

der Kontaktperson	

Name, Funktion und Kontaktdaten der Kontaktperson	-
Beschreibung der Verarbeitung	Hosting

PLANIT// PRIMA

Export vom 29.11.2023

konfidal GmbH
Technisch Organisatorische Maßnahmen

Datenschutzdokumente für die Filzfabrik Wurzen GmbH

Technische und organisatorische Maßnahmen (TOMs)

1.	**Übersicht der zur Datenverarbeitung eingesetzten IT-Systeme**
1.1	**Eingesetzte Hardware** ■ folgende externen Rechenzentren: Datacenter-Parks der Hetzner Online GmbH in Nürnberg, Falkenstein und Helsinki
1.2	**Eingesetzte Software** konfidal Whistleblower Software
2.	**Technische und organisatorische Sicherheitsmaßnahmen**
2.1	**Zutrittskontrolle**
	Technische Maßnahmen
	Perimetersicherung ■ andere: Siehe TOM-Konzept Hetzner Online GmbH
	Gebäudesicherung ■ andere: Siehe TOM-Konzept Hetzner Online GmbH
	Innenraumsicherung ■ andere: Siehe TOM-Konzept Hetzner Online GmbH. Eine Remote-Arbeitsplatz-Regelung ist vorhanden.
	Organisatorische Maßnahmen
	■ andere: Siehe TOM-Konzept Hetzner Online GmbH. Eine Remote-Arbeitsplatz-Regelung ist vorhanden.
2.2	**Zugangskontrolle**
	Technische Maßnahmen

- zentrale Steuerung von Berechtigung (z.B. per Verzeichnisdienst und Identitätsmanagement)
- Benutzeranmeldung mit Kennung und Passwort
- passwortgeschützter Bildschirmschoner
- Zugangsprotokollierung
- Softwarefirewall
- Hardwarefirewall
- keine Administrator-Konten für normale Nutzer
- Sperrung von Clients bei Inaktivität
- andere:
  - Jeglicher Zugriff auf andere Systeme geschieht über eine SSH Verbindung
  - Automatischer Ablauf von Benutzerrechten nach festgelegtem Zeitraum

2.2.2 Organisatorische Maßnahmen

- Berechtigungskonzept
- Passwortregelung
- Routine zur Passworterneuerung
- Passwortrichtlinie (zu Komplexität, Änderung und Geheimhaltung)
- restriktive Vergabe von Admin-Rechten auf Clients
- Routine zur Kontrolle der Rechtevergabe
- Mitarbeiterschulung
- Zentrale Auswahl und Beschaffung von Hard- und Software (Zwecks Kompatibilität, Gewährleistung von Mindeststandards)
- IT-Richtlinie (z.B. zur Installation von Fremdsoftware, zum Umgang mit Mails mit unbekanntem Absender)
- Patch-und Änderungsmanagement für Software; Sicherstellung der Patchverträglichkeit auf Testsystemen vor dem Produktivbetrieb
- andere:
  - Verpflichtende Nutzung eines Passwortmanagers
  - Passwortmanager Accounts sind bei befristeten Mitarbeitern befristet konfiguriert
  - Alle Rechner der konfidal GmbH sind mit starken Passwörtern geschützt
  - Alle RSA Schlüssel sind Passwortgeschützt
  - Alle Passwörter zur konfidal App werden von den Nutzern (Auftragnehmer) selbst erstellt und sind konfidal nicht bekannt. Der Auftraggeber/die Auftraggeberin setzt zusätzliche eigene Maßnahmen zur Zugangskontrolle um

2.3	**Zugriffskontrolle**
	Technische Maßnahmen
	■ zentrale Steuerung von Berechtigung, z.B. durch Verzeichnisdienst ■ Zugriffsprotokollierung ■ Verschlüsselung von Massenspeichern ■ Pseudonymisierung von Daten und getrennte Aufbewahrung des Zuordnungsschlüssels ■ andere
2.3.2	**Organisatorische Maßnahmen**
	■ Passwortregelung ■ Berechtigungskonzept ■ Rechteverwaltung durch eine minimale Gruppe von Administratoren ■ Routine zur Kontrolle der Rechtevergabe
2.4	**Weitergabekontrolle**
	Technische Maßnahmen
	■ zentrale Steuerung von Berechtigung ■ SSL-Verschlüsselung bei Web-Access ■ Pseudonymisierung von Daten ■ Protokollierung von Datenübermittlungen ■ Sicherung gegen Verkehrsflussanalyse (Traffic Flow Confidentiality) bei Übermittlung von Daten mit hohem Schutzbedarf über öffentliche Netze ■ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form ■ sichere Löschung von Datenträgern vor Wiederverwendung
	Organisatorische Maßnahmen
	■ Berechtigungskonzept ■ Dokumentation der Empfänger von Daten und der Zeitspanne der geplanten Überlassung bzw. vereinbarte Löschfristen ■ Mitarbeiterschulung ■ Richtlinie zur Aufbewahrung, Löschung und Sperrung personenbezogener Daten
2.5	**Eingabekontrolle**
	Technische Maßnahmen

	■ zentrale Steuerung von Berechtigung, z.B. durch Verzeichnisdienst ■ personenscharfe Nutzerkonten ■ Eingabeprotokollierung
2.5.2	**Organisatorische Maßnahmen**
	■ Passwortregelung ■ Berechtigungskonzept ■ personenscharfe Nutzerprofile ■ Mitarbeiterschulung
2.6	**Auftragskontrolle**
	Technische Maßnahmen
	■ zentrale Steuerung von Berechtigung, z.B. durch Verzeichnisdienst ■ Protokollierung von Systemzugriffen
2.6.2	**Organisatorische Maßnahmen**
	■ Auswahl von Auftragnehmern nach definierten Sorgfaltsgesichtspunkten
2.7	**Verfügbarkeitskontrolle**
	Technische Maßnahmen
	■ andere: Siehe TOM-Konzept Hetzner Online GmbH
	Organisatorische Maßnahmen
	■ Backup-Konzept ■ Routine zur Warnung bei akuten Bedrohungen ■ Mitarbeiterschulung ■ Recovery-Konzept ■ Recovery-Tests
2.8	**Trennungskontrolle**
	Technische Maßnahmen

- ■ logisch getrennte Speicherung
- ■ Trennung von Produktiv- und Testsystem
- ■ einheitliche Verschlüsselung von Daten, die zu einem Zweck verarbeitet werden

Organisatorische Maßnahmen

- ■ Mitarbeiterschulung
- ☐ Kennzeichnen von Datensätzen mit Zweckattributen (Tagging
- ■ Rechtevergabe nach Need-To-Know-Prinzip (Least Privilege Model)
- ■ Richtlinien für Softwaretests
- ☐ andere

2.9 Pseudonymisierung und Verschlüsselung

- ■ Pseudonymisierung, nämlich:
  Bei der programmatischen Weiterverarbeitung von Daten in der konfidal App werden Pseudonyme und keine personenbezogenen Identifizierungen verwendet.

  Für die Pseudonymisierung der von Nutzern in der App verarbeiteten Daten ist der Auftraggeber/die Auftraggeberin verantwortlich.

- ■ Verschlüsselung von ruhenden Daten, nämlich
- ■ Verschlüsselung von Daten beim Transport über interne Netze, nämlich: RSA
- ■ Verschlüsselung von Daten beim Transport über öffentliche Netze, nämlich: SSL

2.10 Belastbarkeit der Systeme und Dienste

Technische Maßnahmen

- ■ Server-Cluster für Datenbanken, Webservices und sonstige Dienste
- ■ Redundanz von Systemen und Komponenten
- ■ Vorbereitung auf netzbasierte Angriffe (DDoS-Mitigation)

Organisatorische Maßnahmen

- ■ Monitoring der Systemverfügbarkeit
- ■ Vereinbarung angemessener Service-Level, Reaktions- und Wiederherstellungszeiten mit Dienstleistern
- ■ Überwachung von Service-Leveln

2.11 Rasche Wiederherstellung

Technische Maßnahmen

	■ Backup-Verfahren ■ Spiegelung produktiver Systeme (mit Hot Standby)
	Organisatorische Maßnahmen
	■ Festlegung angemessener Recovery Point Objektives ■ Festlegung angemessener Recovery Time Objektives ■ Planung für Exit / Remigration / Second Level Outsourcing (z.B. Einsatz portabler virtueller Maschinen und standardisierter / dokumentierter APIs)
2.12	**Regelmäßige Überprüfung**
	Technische Maßnahmen
	■ Protokollierung von sicherheitsrelevanten Vorgängen
2.12.2	**Organisatorische Maßnahmen**
	■ Routine zur Überprüfung implementierter Sicherheitsmaßnahmen ■ Auswertung von Sicherheitsvorfällen ■ Auswertung von Protokollen sicherheitsrelevanter Vorgänge

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

- **Zutrittskonstrolle**
  - **Datacenter-Parks in Nürnberg, Falkenstein und Helsinki**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenter-Park
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
  - **Verwaltung**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Videoüberwachung an den Ein- und Ausgängen
- **Zugangskontrolle**
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
    - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem

Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.

- für Managed Server, Webhosting und Storage Share
    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

- **Zugriffskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
    - für Managed Server, Webhosting und Storage Share
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
        - Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.
- **Datenträgerkontrolle**
    - **Datacenter-Parks in Nürnberg, Falkenstein und Helsinki**
        - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
        - Defekte Festplatten, die nicht sicher gelöscht werden können,

werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).

- **Trennungskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
    - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Trennungskontrolle obliegt dem Auftraggeber.
  - für Managed Server, Webhosting und Storage Share
    - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
    - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- **Pseudonymisierung**
  - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

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

- **Weitergabekontrolle**
  - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
  - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- **Eingabekontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

- für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
- für Managed Server, Webhosting und Storage Share
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
        - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
        - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
        - Monitoring aller relevanten Server.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Dauerhaft aktiver DDoS-Schutz.
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Datensicherung obliegt dem Auftraggeber.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Dauerhaft aktiver DDoS-Schutz.
    - Für Managed Server, Webhosting und Storage Share
        - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
        - Einsatz von Festplattenspiegelung.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Einsatz von Softwarefirewall und Portreglementierungen.

- Dauerhaft aktiver DdoS-Schutz.

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**
  - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

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

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- **Auftragskontrolle**
  - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
  - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
  - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

SIGNATUREN & SIEGEL

Zertifizierung von elektronischen Signaturen und Siegeln

Zertifikat für ein Dokument mit Autenti ID: 6695febd-b68e-4dd6-a476-1695f90fba09
erstellt am: 2023-11-29 23:20 (GMT+01:00)

Das von konfidal GmbH martin.meng@konfidal.eu zur Signatur vorgelegte Dokument wurde mit einem elektronischen Siegel vor Änderungen geschützt.

2023-11-29 23:20 (GMT+01:00)

Martin Meng
martin.meng@konfidal.eu
CEO
konfidal GmbH
Steuernummer: 355946845

Elektronische Signatur, die vom Auntenti-Siegel geschützt ist

Authentifizierung: E-mail
Grund: Unterzeichnen des Dokuments

IP-Adresse: 2a02:908:1911:1ca0:813f:83c4:2f9a:8b25
2023-11-29 23:21 (GMT+01:00)

Volkmar Erl
Volkmar.Erl@filzfabrik-wurzen.de
Geschäftsleitung
Filzfabrik Wurzen GmbH

Elektronische Signatur, die vom Auntenti-Siegel geschützt ist

Authentifizierung: E-mail
Grund: Unterzeichnen des Dokuments

IP-Adresse: 217.86.237.2
2023-12-14 13:48 (GMT+01:00)

Elektronische Signaturen, die Authentizität und Integrität des Dokuments nach dem Unterzeichnen sind durch ein elektronisches Siegel geschützt

2023-12-14 13:48 (GMT+01:00)

Dieses Dokument bescheinigt, dass elektronische Signaturen eingereicht wurden.

Die Unterzeichner haben elektronische Signaturen gemäß der Autenti-Regelungen (Inhalt unter: https://autenti.com/en/terms) geleistet und erklärt, dass die zur Identifikation angegebenen Daten richtig und wahr sind. Die Authentifizierung der Unterzeichner hinsichtlich der in der elektronischen Signatur enthaltenen Daten wurde durchgeführt.

Die Dienstleistung wurde in Übereinstimmung mit der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments vom 23. Juli 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS) erbracht.