

Sicherheitsmaßnahmen für die Vernichtung von Datenträger der documentus GmbH Stuttgart

Vorwort

Der ordnungsgemäße Umgang mit Dokumenten und Daten die vertrauliche und sensible Informationen enthalten sind für documentus von höchster Bedeutung. Bei documentus genießen darüber hinaus der Schutz und die Sicherheit sämtlicher Arten personenbezogener Daten eine besondere Beachtung. Sowohl innerhalb des Unternehmens als auch im Rahmen der Auftragsverarbeitung misst documentus dem Schutz der personenbezogenen Daten der Mitarbeiter und der Kunden höchste Aufmerksamkeit bei. In unserem gesamten Unternehmen genießt der Datenschutz unter Einbeziehung personenbezogener und anderer vertraulicher Daten höchste Priorität.

Seit der Veröffentlichung der DIN-SPEC 66399-3 im Februar 2013 ist die Norm *Büro- und Datentechnik – Vernichten von Datenträgern* komplettiert. Diese bildet erstmals den Prozess der Datenträgervernichtung ab, und nimmt dabei sowohl uns als auch unsere Kunden in die Pflicht. Das Inkrafttreten der Datenschutzgrundverordnung (DS-GVO) im Mai 2018 stellt die datenschutzrechtlichen Gegebenheiten neu auf und nimmt insbesondere unsere Kunden und uns als Auftragsverarbeiter ganz besonders in die Pflicht.

Unser Haus ist gemäß der hohen Anforderungen der DIN 66399 als Fachbetrieb für Akten- und Datenträgervernichtung zertifiziert. Das detaillierte Zertifikat der PÜG (Prüf- und Überwachungsgesellschaft mbH) in welchem für jede Datenträgerkategorie die jeweils mögliche Sicherheitsstufe und Schutzklasse aufgelistet ist, senden wir unseren Kunden gerne zu.

Die documentus GmbH Stuttgart, Eisentalstraße 6 in 71332 Waiblingen (im Folgenden documentus) verpflichtet sich die zum Zwecke der Vernichtung übernommenen Datenträger gleich welcher Form unabhängig von deren Schutzbedürftigkeit durch geeignete und anerkannte Verfahren der mechanischen Zerstörung reproduktionssicher zu vernichten.

Wenn uns als Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, melden wir diese dem Verantwortlichen (unserem Kunden) unverzüglich um diesen dabei aktiv zu unterstützen seiner Pflicht nachzukommen und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese seiner zuständigen Aufsichtsbehörde mitzuteilen.

Wir haben nachfolgend näher bezeichneten Datenschutzbeauftragten schriftlich bestellt:

ISICO Datenschutz GmbH
Thomas Weber
Am Hamburger Bahnhof 4
10557 Berlin

Zur Umsetzung datenschutzrechtlicher Forderungen im Unternehmen besitzt er gegenüber der Geschäftsleitung ein direktes Vortrags-, Empfehlungs- und Beratungsrecht. In der Anwendung seiner Fachkunde ist er weisungsfrei.

Unsere Mitarbeiter sind über die einschlägigen Datenschutzvorschriften belehrt. Regelmäßig werden sie durch den Datenschutzbeauftragten und die Datenschutzkoordinatoren über relevante Datenschutzmaßnahmen, Änderungen und Aktualisierungen im Datenschutzrecht geschult. Die Verpflichtungen der Mitarbeiter auf Vertraulichkeit sind aktenkundig.

Weiter sind unsere Mitarbeiter zur Verschwiegenheit über alle Tatsachen verpflichtet, die dem Auftraggeber in Ausübung einer Tätigkeit als Geheimnisträger im Sinne des § 203 Abs. 1 o. 2 StGB (wie etwa: § 43a BRAO, § 18 BnotO, § 39 PAO, § 57 StBerG, § 43 WiPrO) bekannt geworden sind und zu denen der Auftraggeber uns den Zugang eröffnet hat. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Jeder Mitarbeiter ist sich dessen bewusst, dass ihm anvertraute personenbezogene Daten ausschließlich im Rahmen der Zweckbestimmung verwendet werden dürfen und gegen unberechtigten Zugriff gesichert werden müssen.

Es ist die gemeinsame Pflicht von Geschäftsführung, Vorgesetzten und Mitarbeitern das von unseren Kunden erwartete hohe Maß an Sicherheit zu gewährleisten und ständig zu verbessern. Die Einhaltung der Sicherheitsvorgaben und –grundsätzen ist somit die Aufgabe aller Mitarbeiter von documentus.

Einzigster Zweck der Übernahmen von Akten- und Datenmaterial durch die documentus GmbH liegt in deren Vernichtung – in der Sparte documentus-Archiv in deren Einlagerung.

Das Akten- und Datenmaterial wird nur entsprechend den Weisungen des Auftraggebers verarbeitet, diese Verarbeitung entspricht der Vernichtung. Darüber hinaus werden die (Sozial)daten nicht anderweitig genutzt (Auftragskontrolle).

Sämtliche übernommene Datenträger werden standardgemäß nach der entsprechenden Sicherheitsstufe 3 vernichtet. Auf Wunsch ist auch eine Vernichtung der Datenträger nach einer höheren Sicherheitsstufe möglich. Die Vernichtung von magnetischen Datenträgern, Festplatten und elektronischen Datenträgern (T, H und E) kann bis zur Sicherheitsstufe 5 gewährleistet werden. Unabhängig von der gewünschten Partikelgröße des Shreddergutes arbeiten wir ab der Übernahme der Datenträger nach den strengen Vorgaben der Schutzklasse 2, oder auf Kundenwunsch nach der Schutzklasse 3.

Der Transport der Datenträger erfolgt in verschlossenen Sicherheitsbehältern, bzw. Sicherheitscontainern. Unsere Fahrzeuge sind mit einem aktiven GPS-System ausgestattet. Die Vernichtung der Datenträger erfolgt ausnahmslos in einem Sicherheitsbereich auf dem Firmengelände der documentus GmbH gemäß den folgenden Datensicherungsmaßnahmen unter Beachtung der Datenschutzgrundverordnung und der DIN 66399.

1. Zutrittskontrolle und Sicherung des Sicherheitsbereichs

1.1. Der Zugang zum Sicherheitsbereich für die Vernichtung von vom Kunden überlassenen Datenträger ist sowohl für Personen als auch für Fahrzeuge nur durch gesicherte Eingänge möglich.

Der Zugang für Personen in den Sicherheitsbereich ist nur mittels eines Chips möglich mit welchem sich der Berechtigte als solcher ausweist (**Zutrittskontrolle**). Die Überprüfung der Zugangsberechtigung erfolgt über den Zentralrechner. Tore und

Andockstationen für LKW können nur von berechtigtem Personal vom Inneren des Sicherheitsbereiches geöffnet werden.

- 1.2. Alle Türen oder Tore, die direkt in die Sicherheitszone führen, schließen automatisch bzw. offene Türen/Tore werden durch optische oder akustische Meldeeinrichtungen angezeigt.
- 1.3. Sind Türen oder Tore, die direkt in die Sicherheitszone führen, über die vorgesehene Zeitdauer hinaus offen, so erfolgt eine automatische Meldung an den örtlichen Sicherheitsverantwortlichen.
- 1.4. Der Sicherheitsbereich unterliegt einer visuellen Überwachung (Videoüberwachung), die gewährleistet, dass der Sicherheitsbereich ständig und ohne Zeitverzug überwacht werden kann. Die aufgezeichneten Daten werden gespeichert.
- 1.5. Außerhalb der Betriebszeiten ist der Sicherheitsbereich durch eine Einbruchmeldeanlage gesichert, die im Fall eines unberechtigten Zutritts eine Hilfe leistende Stelle alarmiert. Gleichzeitig wird eine Videoanlage aktiviert, welche in der Lage ist auch bei Dunkelheit aufzuzeichnen.
- 1.6. Der Sicherheitsbereich in welchem Datenmaterial abgeladen, für die Vernichtung vorbereitet und vernichtet wird, ist in massiver Bauausführung erstellt, und ist baulich so gestaltet, dass Datenmaterial nicht unkontrolliert nach außen gelangen kann. Türen, Fenster, Tore und der Gleichen sind so abgesichert, dass Datenmaterial nicht herausgedrückt oder –geweht werden kann. Für die Einbringung von unvernichteten Datenträgern in die Sicherheitszone steht eine Schleuse oder Andockstation (für Fahrzeuge) zur Verfügung.
- 1.7. Im Sicherheitsbereich erfolgt ausschließlich die Vernichtung von Datenträgern, die Verarbeitung von anderen Wertstoffen erfolgt in örtlich getrennten Räumlichkeiten bei der Muttergesellschaft, der ALBA Süd GmbH & Co.KG.

2. Transport und Transportbehälter (Weitergabekontrolle)

- 2.1. Für die Abholung und den Austausch der Sicherheitsbehälter beim Kunden und für die Vernichtung von Datenträgern werden keine Subunternehmen eingesetzt. Der Transport der Sicherheitsbehälter erfolgt ausschließlich durch die Firma documentus GmbH die Fahrer haben keinen direkten Zugriff auf die Schlüssel der gefüllten Sicherheitsbehälter. Für die Sammlung, Lagerung und den Transport von Datenträgern werden dem Schutzbedarf angemessene geschlossene und verschlossene Sicherheitsbehälter eingesetzt.
- 2.2. Sämtliche Fahrzeuge sind mit einem aktiven GPS-Ortungssystem ausgestattet.
- 2.3. Die Transportfahrzeuge für rollbare Sicherheitsbehälter verfügen ausschließlich über einen geschlossenen, Sicherheitsaufbau und Hebebühne. Das Fahrzeug bleibt während des Transports von Datenmaterial nicht ohne qualifizierte Aufsicht, bzw. wird während

des Be- und Entladevorgangs beim Kunden vor Ort nach jeder Be- und Entladung verschlossen.

- 2.4. Die Übernahme der Datenträger bzw. der Sicherheitsbehälter wird in einem Übernahmeprotokoll dokumentiert. Dieses enthält unter anderem folgende Angaben: Name Übernehmender (Fahrer), Name Übergebender (Kunde), Fahrzeugkennung, Art und Anzahl der Datenträger (z.B. Behältertyp) sowie Datum, Uhrzeit und Ort der Übernahme.
- 2.5. Datenträgermaterial wird ausschließlich in den dafür vorgesehenen Sicherheitsbehälter transportiert (Ausnahme: Monoladungen eines Kunden, nach Absprache), so dass eine Verwechslung zwischen Datenträgern und sonstigen Altpapieren nicht möglich ist.
- 2.6. Die eingesetzten Sicherheitsbehälter bzw. Sicherheitscontainer sind abschließbar. Die Sicherheitsbehälter DC240 und DC350 verfügen über einen Einwurfschlitz und können mit sogenannter Z-Schließung angeboten werden, bei diesem System verfügt jeder einzelne Behälter über einen eigenen Schlüssel. Der Schlüssel bleibt ständig beim Behälter, dadurch wird u.a. gewährleistet, dass z.B. Mitarbeiter einer Abteilung nicht Behälter einer anderen Abteilung öffnen können.
- 2.7. Die Lagerung (bis zur Vernichtung) und Entleerung der Sicherheitsbehälter findet ausschließlich innerhalb eines geschlossenen und überwachten Sicherheitsbereichs statt.
- 2.8. Nach der Behälterentleerung im documentus-Betrieb wird an jeden Behälter ein Kontrollbeleg angebracht, um eine vollständige Entleerung und Behälterprüfung anzuzeigen, dadurch ist das Ziel der Rückverfolgbarkeit der Entleerungskontrolle erreicht. Der für die Entleerung Verantwortliche dokumentiert seine Tätigkeit auf dem Schichtbericht mit den verwendeten Kontrollbelegnummern und seiner Unterschrift.

3. Personal

- 3.1. Es werden ausschließlich Personen beschäftigt die schriftlich zur Vertraulichkeit verpflichtet sind. Das Personal wird weiter darüber belehrt, dass Verstöße gegen das Datengeheimnis (z.B. §§ 80/85 SGB und §§ 203/204 StGB) mit Freiheits- oder Geldstrafen geahndet werden können.
- 3.2. Das eingesetzte Personal legt der documentus GmbH bei Arbeitsaufnahme (Einstellung) ein Führungszeugnis vor, es darf keine für die Durchführung einer Auftragsverarbeitung relevanten Eintragungen enthalten. Zu diesen relevanten Eintragungen gehören unter anderem die Tatbestände Betrug und Diebstahl usw. Das Führungszeugnis ist alle drei Jahre neu vorzulegen.
- 3.3. Das Personal weist sich beim Kunden durch einen firmeneigenen Sicherheitsausweis mit Lichtbild aus.
- 3.4. documentus Stuttgart, setzt für regionale Kunden zur Auftrags Erfüllung für Transport, Handling und Vernichtung keine weiteren Auftragsverarbeiter (Subunternehmer) ein. Bei

überregionalen Kunden werden ausschließlich documentus-Partner zur Auftragserfüllung eingesetzt.

- 3.5. Die documentus GmbH verpflichtet alle beschäftigte Personen, jedes Beiseiteschaffen von Datenmaterial sowie die Einblicknahme in dieses und eine, wie auch immer geartete, sonstige Verwendung zu unterlassen. Die documentus GmbH überwacht die Einhaltung dieser Vorschriften, z.B. durch Videoüberwachung.

3. Vernichtung der Datenträger (Auftragskontrolle)

- 4.1. Die Vernichtung der Datenträger erfolgt in der Regel taggleich, spätestens jedoch innerhalb von 24 Stunden. Datenträger der Schutzklasse 3 (Sicherheitsstufe 4) werden taggleich vernichtet. Bis unmittelbar vor der Vernichtung bleiben die Sammelbehälter verschlossen. Mit der Abrechnung erhält der Kunde über jede einzelne Abholung ein Vernichtungszertifikat, dieses enthält u.a. folgende Daten: Tag der Übernahme der Datenträger beim Kunden, Tag der Materialannahme im Datensicherheitsbereich, Tag der Vernichtung der übernommenen Datenträger. Art und Menge der übernommenen Datenträger, sowie die jeweilige Sicherheitsstufe und Schutzklasse.

- 4.1. Es werden sechs Arten von Datenträgern unterschieden, diesen Datenträgern sind als Kennung Buchstaben zugeordnet (PFOTHE). Beispiele für die einzelnen Datenträgerarten sind nachfolgend in Klammern dargestellt:

- P:** Informationsdarstellung in Originalgröße (Papier, Ordner, Listen)
- F:** Informationsdarstellung verkleinert (Mikrofilm, Mikrofiches)
- O:** Informationsdarstellung auf optischen Datenträgern (CD, DVD)
- T:** Informationsdarstellung auf magnetischem Datenträger (Disketten)
- H:** Informationsdarstellung auf Festplatten mit magnetischem Datenträger
- E:** Informationsdarstellung auf elektronischen Datenträgern (Chipkarte)

- 4.2. Die Vernichtung der Datenträger **P**, **F**, **O**, und **E** erfolgt standardgemäß nach DIN 66399 nach der jeweiligen Sicherheitsstufe 3 – also zum Beispiel bei Papierdatenträger nach der Sicherheitsstufe **P-3**. Die Vernichtung von Datenträgern der Kategorie **T** erfolgt standardgemäß nach der Sicherheitsstufe **T-4**.

- 4.3. Die in 4.2. genannten Datenträger können auf Kundenwunsch und gegen Aufpreis auch gemäß der jeweiliges nächst höheren Sicherheitsstufe vernichtet werden.

- 4.4. Wegen der Vielfalt der aufgezeichneten Daten erfolgt die Vernichtung von Festplatten mit magnetischen Datenträgern (z.B. Festplatten aus Laptops, Computern oder Servern) aus Sicherheitsgründen gemäß der Sicherheitsstufe **H-4**. Auf Wunsch ist hier auch eine Vernichtung nach Sicherheitsstufe **H-5** möglich.

- 4.5. Bei Datenträgern mit Informationsdarstellung in Originalgröße welche nach Schutzklasse drei vernichtet werden wird der Inhalt der eingesetzten Sicherheitsbehälter direkt der Zerkleinerungsanlage zugeführt, der Schüttvorgang wird videoüberwacht und aufgezeichnet. Die Zuführung zur Zerkleinerungsmaschine bei Datenträgern mit

Informationsdarstellung in Originalgröße welche gemäß der Schutzklasse zwei vernichtet werden, erfolgt über ein videoüberwachtes Förderband.

- 4.6. Zur Sicherstellung und Aufrechterhaltung der durch die DIN 66399 vorgegebenen Partikelgrößen werden wöchentlich Materialproben aus der laufenden Produktion entnommen und deren Partikelgröße ausgewertet. Halbjährlich wird gemäß DIN 66399 ein Prüfzeugnis für die Partikelgrößen aller Datenträgerkategorien erstellt. Diese Prüfzeugnisse sind Bestandteil des mindestens alle zwei Jahre stattfindenden Rezertifizierungsprozesses.

5. Organisation

- 5.1. Es erfolgt eine lückenlose Protokollierung der Abholung der Sicherheitsbehälter beim Kunden, der Ankunft der Datenträger im Sicherheitsbereich, der erfolgten Vernichtung des Datenmaterials und der Bestätigung der Vernichtung (Zertifikat) mit Angabe von Datum und Nennung der verantwortlich handelnden Person.
- 5.2. Es wurden organisatorische Maßnahmen getroffen um eine Verwechslung von Altpapieren und Papierdatenträger auszuschließen. So werden übernommene Papierdatenträger in den dafür vorgesehenen Sicherheitsbehälter der Typen DC240 bis DC660, bzw. in Sicherheitsmulden DC10 und Sicherheitscontainern DC28 übernommen. Eventuell übernommenes Mischpapier wird in andersartigen Behältnissen übernommen.
- 5.3. Es wurden organisatorische Maßnahmen zur Kennzeichnung derjenigen Sicherheitsbehälter getroffen deren Inhalt nach einer höheren Sicherheitsstufe als der Sicherheitsstufe 3 oder nach der Schutzklasse 3 vernichtet werden muss.
- 5.4. Die documentus GmbH hat ein Qualitätsmanagementsystem nach DIN EN ISO 9001:2015 eingeführt und ist als Entsorgungsfachbetrieb (EfB) zertifiziert. Betriebsabläufe und Verantwortlichkeiten sind in schriftlichen Organisations-, Verfahrens- und Arbeitsanweisungen dargestellt. Diese qualitätssichernden Aktivitäten werden in Übereinstimmung mit den betreffenden Anforderungen aus den Normen und anderen normativen Richtlinien gesteuert und überwacht. Diese Steuerung und Überwachung erfolgt ständig im Rahmen der Führungsverantwortung der Vorgesetzten und durch interne Qualitätsaudits. In letzter Konsequenz trägt aber jeder Mitarbeiter von documentus durch sein persönliches Verhalten zur Produktqualität des Unternehmens bei.

Wie in der QMV festgelegt, erfolgt mindestens einmal jährlich eine Innensicherheitsrevision durch documentus Deutschland. Alle qualitätsrelevanten Abläufe, Einrichtungen und Personen werden durch das Qualitätsmanagement erfasst und überwacht.

- 5.5. Die documentus GmbH hat einen Beauftragten für den Datenschutz bestellt. Im Übrigen unterliegt die documentus GmbH und deren Mitarbeiter u.a. den gesetzlichen Bestimmungen der Datenschutzgrundverordnung (DSGVO), des Strafgesetzbuches (StGB) sowie dem Sozialgesetzbuch (SGB).

- 5.6. Die documentus GmbH Stuttgart ist als Fachbetrieb Akten- und Datenvernichtung gemäß DIN 66399 zertifiziert, sowie zertifizierter Entsorgungsfachbetrieb, weiter wurde nach DIN ISO ein Qualitätsmanagementsystem etabliert. Zur Überprüfung der getroffenen Maßnahmen werden zusätzlich interne Audits durchgeführt.
- 5.7. Kommt es z.B. durch Brand oder sonstigen Ereignissen zu einer Beschädigung der Vernichtungsanlage, welche zur Folge hat, dass eine ordnungsgemäße Vernichtung der Datenträger im documentus-Betrieb in Waiblingen nicht weiter möglich ist, sind gemäß Notfallkonzept mit den angrenzenden documentus-Betrieben in Bayern und Hessen Vereinbarungen dahingehend getroffen, dass das zu Vernichtende Material in diesen Betrieben angedient und dort vernichtet werden kann. Das Notfallkonzept enthält zusätzlich präventive Maßnahmen und Vorschriften zur Verhütung von Ereignissen welche zu einem teilweisen oder vollständigen Ausfall der Anlage führen könnten.
- 5.8. Kommt es durch einen Unfall oder sonstigen Vorkommnissen dazu, dass ein documentus Hebebühnenfahrzeug mit Sicherheitsaufbau seine geplante Tour nicht fortsetzen kann sind die einzuleitenden Maßnahmen in einem entsprechenden Prozessablauf („Prozessablauf Unfall oder Defekt Hebebühnenfahrzeug“) geregelt.

6. Sonstiges

- 6.1. **Energiepolitik:** Als Teil der ALBA Group trägt die documentus GmbH Stuttgart mit ihren unternehmerischen Tätigkeiten aus den Bereichen Recycling, Aufarbeitung und Rohstoffhandel maßgeblich zu einem nachhaltigen Umgang mit natürlichen Ressourcen bei und leistet einen wertvollen Beitrag zur Senkung der CO₂-Emissionen.
- 6.2. **Recycling** Alle von uns übernommenen Papierdatenträger werden nach der datenschutzkonformen Vernichtung dem Recyclingkreislauf zugeführt. Zu unseren Abnehmern gehören insbesondere Papierfabriken im Bereich der Hygienepapierherstellung.
- 6.3. **Unser Verhaltenskodex:** Die Basis unseres Handels ist der Verhaltenskodex (Code of conduct) der ALBA Group. Als Leitlinie benennt er die Mindeststandards für den Umgang untereinander, aber auch mit Geschäftspartnern und der Öffentlichkeit. Dazu gehört in erster Linie, dass wir die gesetzlichen Vorgaben kennen – und diese einhalten. So achten, schützen und fördern wir zum Beispiel die weltweit geltenden Menschenrechte und garantieren die freie Entfaltung der Persönlichkeit. Wir behandeln alle Menschen gleich, ungeachtet Ihres Geschlechts, Alters, Ihrer Hautfarbe, Kultur, ethnischer Herkunft, Religionszugehörigkeit, Weltanschauung, sexuellen Identität oder möglichen Behinderungen. Im Mittelpunkt unserer täglichen Arbeit stehen neben den datenschutzrechtlichen Vorgaben, Umweltschutz und Nachhaltigkeit, sowie die Sicherheit und Gesundheit unserer Mitarbeiterinnen und Mitarbeiter.

7. Datensicherheitskonzept

Der AN realisiert folgende technischen und organisatorische Maßnahmen.

a) Zutrittskontrolle

	Dienstleistung	
	Archivierung	Vernichtung
Zutrittssicherung an allen Zutrittsmöglichkeiten zum Sicherheitsbereich	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Verzeichnis zur Verwaltung und Vergabe der individuellen Zutrittsberechtigungen zum Sicherheitsbereich	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Einbruchmeldeanlage gegen unbefugten Zutritt zum Sicherheitsbereich	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zutrittsschleusen in den Sicherheitsbereich für Personen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zufahrtsschleusen oder gesicherte Andockschleusen für LKW an den Zufahrten/Zugängen in den Sicherheitsbereich	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Optische oder akustische Meldung an den örtlichen Sicherheitsbeauftragten, wenn Zugänge zum Sicherheitsbereich über eine bestimmte Zeit hinaus offen sind		<input checked="" type="checkbox"/>
Zutritt von Mitarbeitern in den Sicherheitsbereich nur mit zutrittsberechtigtem ID-Chip/Schlüssel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zutritt betriebsfremder Personen nur nach vorheriger Identifikation über z.B. Personalausweis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zutritt betriebsfremder Personen in den Sicherheitsbereich nur nach Unterzeichnung einer Belehrung-/Verpflichtungserklärung	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zutritt betriebsfremder Personen in den Sicherheitsbereich nur in ständiger Begleitung eines zutrittsberechtigten Mitarbeiters	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dokumentation der Zutritte betriebsfremder Personen in den Sicherheitsbereich anhand einer Besucherliste/eines Besucherverzeichnisses	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dokumentation aller Zutritte zum Sicherheitsbereich mittels Videoüberwachung	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

b) Zugangskontrolle

	Dienstleistung	
	Archivierung	Vernichtung
Vergabe individueller Zutrittsberechtigungen zum Sicherheitsbereich für Mitarbeiter	☑	☑
Zutritt betriebsfremder Personen nur nach vorheriger Identifikation über z.B. Personalausweis	☑	☑
Dokumentation der Zutritte zum Sicherheitsbereich mittels Videoüberwachung	☑	☑
Dokumentation der Aktivitäten im Sicherheitsbereich mittels Videoüberwachung		☑
Verbot von Foto- und Filmaufnahmen im Sicherheitsbereich	☑	☑
Einbruchmeldeanlage im Sicherheitsbereich	☑	☑

c) Zugriffskontrolle

	Dienstleistung	
	Archivierung	Vernichtung
Verpflichtung aller Mitarbeiter auf alle einschlägigen und relevanten Gesetze	☑	☑
Verwaltung und Dokumentation der Vergabe von Schlüsseln, ID-Chips und Schließberechtigungen an Betriebsangehörige	☑	☑
Sorgfältige Auswahl und fortlaufende Kontrolle der Mitarbeiter (u.a. Vorlage polizeilicher Führungszeugnisse)	☑	☑
Transport von zu vernichtenden Akten und Datenträgern grundsätzlich in ge- und verschlossenen Sicherheitsbehältern		☑
Dokumentation abgeholter und angelieferter Sicherheitsbehälter anhand von Lieferscheinen (in digitaler Form oder Papierform)	☑	☑
Überwachung und Dokumentation der LKW-Positionen anhand GPS-Verfolgung		☑
Durchführung interner Audits und externer Revisionen	☑	☑

d) Maßnahmen zur Sicherstellung von Integrität

	Dienstleistung	
	Archivierung	Vernichtung
Transport von zu vernichtenden Akten und Datenträgern grundsätzlich in ge- und verschlossenen Sicherheitsbehältern oder in speziellen Sicherheitspresswagen/-LKW		<input checked="" type="checkbox"/>
Transport von Sicherheitsbehältern/Kartonagen ausschließlich in geschlossenen Fahrzeugen mit festem Aufbau	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dokumentation abgeholter und angelieferter Sicherheitsbehälter anhand von Lieferscheinen (in digitaler Form oder Papierform)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Überwachung und Dokumentation der LKW-Positionen anhand GPS-Verfolgung		<input checked="" type="checkbox"/>
Arbeitsanweisungen gemäß dem documentus Qualitätsmanagementsystem zur Sicherstellung der Integrität	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
regelmäßige Schulung aller Mitarbeiter auf die in ihrem Arbeitsbereich wichtigen, datenschutzrelevanten Aspekte bei der Auftragsdurchführung	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sicherheitskontrollstreifen zur Dokumentation der vollständigen Entleerung der Sicherheitsbehälter im Sicherheitsbereich		<input checked="" type="checkbox"/>
Zertifizierung gemäß DIN 66399		<input checked="" type="checkbox"/>
Zertifizierung gemäß ISO 9001:2015	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

e) Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

	Dienstleistung	
	Archivierung	Vernichtung
Verpflichtung aller documentus Partner zur Einhaltung der documentus Sicherheitsstandards	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Verpflichtung aller documentus Partner zur Einhaltung der DIN 66399		<input checked="" type="checkbox"/>
Einbruchmeldeanlage im Sicherheitsbereich	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notfallplanung zur Prävention und Bewältigung von Notfällen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Regelungen zur Risikoidentifikationen, Risikobewertungen, Risikominimierung und Risikobewältigung gemäß ISO 9001:2015	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vorhaltung redundanter Anlagentechnik innerhalb der documentus Gruppe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

f) Maßnahmen zur Sicherstellung der Belastbarkeit

	Dienstleistung	
	Archivierung	Vernichtung
Notfallplanung zur Prävention und Bewältigung von Notfällen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
redundante Anlagentechnik innerhalb der documentus Gruppe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Regelungen zur Risikoidentifikationen, Risikobewertungen, Risikominimierung und Risikobewältigung gemäß ISO 9001:2015	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

g) Maßnahmen zur Gewährleistung der Wirksamkeitskontrolle

	Dienstleistung	
	Archivierung	Vernichtung
Verfahren für regelmäßige Kontrollen/Audits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Definition von Prozessen und Arbeitsanweisungen zur Sicherstellung der vertraglich vereinbarten Leistungen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zertifizierung gemäß DIN 66399		<input checked="" type="checkbox"/>
Zertifizierung gemäß ISO 9001:2015	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Durchführung interner Audits und externer Revisionen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

h) Weisungskontrolle bzw. Auftragskontrolle

	Dienstleistung	
	Archivierung	Vernichtung
Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO mit den gesetzlich geforderten Regelungen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Verwendung von Papier-/und oder digitalem Lieferschein mit Angabe von Art und Menge abgeholter, geleerter oder angelieferter Sicherheitsbehälter/Kartonagen, sowie Angabe von Datum, Lieferanschrift, Name des Mitarbeiters und Name des Kunden	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unterschrift des Kunden auf dem Lieferschein (in digitaler Form oder in Papierform)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Erstellung eines Vernichtungsprotokolls gemäß DIN SPEC 66399-3		<input checked="" type="checkbox"/>
Überwachung und Dokumentation der LKW-Positionen anhand GPS-Verfolgung		<input checked="" type="checkbox"/>
Verpflichtung aller Mitarbeiter auf alle einschlägigen und relevanten Gesetze	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>