

DIN EN 15713



ICS 13.310

Entwurf

Einsprüche bis 2022-05-25
Vorgesehen als Ersatz für
DIN EN 15713:2009-08

**Sichere Vernichtung von vertraulichen Unterlagen –
Verfahrensregeln;
Deutsche und Englische Fassung prEN 15713:2022**

Secure destruction of confidential material –
Code of practice;
German and English version prEN 15713:2022

Destruction sécurisée de documents confidentiels –
Code d'usages;
Version allemande et anglaise prEN 15713:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-03-25 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 81 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 15713:2022) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat von BSI (Vereinigtes Königreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 043-04-51 AA „Vernichten von Datenträgern“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN EN 15713:2009-08 wurden folgende Änderungen vorgenommen:

- a) Dokument fachlich grundsätzlich überarbeitet;
- b) normative Verweisungen aktualisiert;
- c) Literaturhinweise hinzugefügt;
- d) Dokument redaktionell überarbeitet.

Titel de: Sichere Vernichtung von vertraulichen Unterlagen — Verfahrensregeln

Titel en: Secure destruction of confidential material — Code of practice

Titel fr: Destruction sécurisée de documents confidentiels — Code d'usages

Inhalt

	Seite
Europäisches Vorwort.....	4
1 Anwendungsbereich.....	5
2 Normative Verweisungen	5
3 Begriffe und Abkürzungen	6
4 Schutzklasse.....	9
4.1 Allgemeines.....	9
4.2 Bestimmung der Schutzklasse	9
5 Bestimmung der Sicherheitsstufe.....	10
5.1 Allgemeines.....	10
6 Erhöhung der Sicherheitsstufe	11
6.1 Allgemeines.....	11
7 Vernichtungsausrüstung	11
7.1 Allgemeines.....	11
7.2 Verwendung von Vernichtungsausrüstung	12
7.3 Bedienungsanleitung.....	12
7.4 Ergebnis der Vernichtung.....	12
7.5 Bestätigung des Vernichtungsprozesses und dessen Abschluss.....	12
7.6 Wartung und Leistungsüberwachung	13
7.7 Häufigkeit der Bewertung von Vernichtungsausrüstung.....	13
7.8 Redundanz von Vernichtungsausrüstung	14
8 Gelände des Unternehmens für die Vernichtung und Lagerstellen des Dienstleisters.....	14
8.1 Gesicherte Bereiche auf dem Gelände für die Vernichtung und in den Lagerstellen des Dienstleisters.....	14
8.2 Sicherheit.....	15
9 Kontrolle des Zugriffs	16
9.1 Allgemeines.....	16
9.2 Autorisierung des Zugriffs von Unternehmensmitarbeitern.....	16
9.3 Begleiteter Zugriff für Unternehmensmitarbeiter ohne entsprechende Schulung.....	17
9.4 Zugang zu gesichertem Bereich für Besucher und Auftragnehmer	17
9.5 Durchführung der Kontrolle des Zugriffs.....	17
9.6 Anforderungen an die Zugriffsstufe	18
10 Vertrag.....	18
10.1 Allgemeines.....	18
11 Aufzeichnung des Sammelprozesses bis zur Vernichtung.....	19
11.1 Allgemeines.....	19
11.1.1 Aufzeichnung der Übergabe von vertraulichen und sensiblen Unterlagen	19
11.1.2 Vernichtungsnachweis	20
12 Unterauftragsvergabe.....	20
12.1 Allgemeines.....	20
13 Mitarbeiter des Unternehmens	21
13.1 Vertraulichkeitsvereinbarung.....	21
13.2 Sicherheitsüberprüfung der Mitarbeiter	21

13.3	Schulung der Mitarbeiter	21
13.4	Kontrolle der Fahrer des Unternehmens	22
14	Sammlung und Transport von vertraulichen und sensiblen Unterlagen	23
14.1	Allgemeines	23
14.2	Mobile Fahrzeuge zum Schreddern und zur Abholung	23
14.3	Sicherheitsbehälter	24
14.4	Aktenvernichterbeutel	24
15	Lagerung und Aufbewahrung von vertraulichen und sensiblen Unterlagen in der Vernichtungsanlage	24
15.1	Allgemeines	24
16	Planung der Aufrechterhaltung der Betriebsfähigkeit und Reaktion auf Sicherheitsvorfälle	24
16.1	Allgemeines	24
17	Aufbewahrung von Aufzeichnungen	25
17.1	Allgemeines	25
18	Kategorien von vertraulichen und sensiblen Unterlagen	26
18.1	Allgemeines	26
19	Abfallbeseitigung des Endprodukts	26
19.1	Allgemeines	26
20	Lieferkette	27
20.1	Kritische Lieferanten	27
21	Informationssicherheit	27
21.1	Allgemeines	27
Anhang A (informativ) Tabellen zu Ergebnissen der Vernichtung		28
Anhang B (normativ) Sicherer Vernichtungsprozess		35
Literaturhinweise		40

Europäisches Vorwort

Dieses Dokument (prEN 15713:2022) wurde vom Technischen Komitee CEN/TC 263 „Sichere Aufbewahrung von Geld, Wertgegenständen und Datenträgern“ erarbeitet, dessen Sekretariat von BSI gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN 15713:2009 ersetzen.

Gegenüber der vorherigen Ausgabe wurden folgende technische Änderungen vorgenommen:

Dieses Dokument wurde fachlich überarbeitet, damit es eine Benchmark für angemessene Prozesse und Verfahren liefert, die allen Personen oder jeder Organisation zur Verfügung stehen, die vertrauliche oder sensible Unterlagen sicher vernichten möchten, wenn diese nicht mehr benötigt werden.

Dieses Dokument soll für Objekte anwendbar sein, die zum Sicherstellen der Produkt- oder Markenintegrität vernichtet werden müssen.

In diesem Zusammenhang bedeutet „sichere Vernichtung“, dass jedes Objekt oder jeder Datenträger, der vertrauliche oder sensible Daten enthält, derart vernichtet werden muss, dass eine Reproduktion der darauf wiedergegebenen Informationen unmöglich ist oder nur mit erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist.

1 Anwendungsbereich

Dieses Dokument gibt Empfehlungen und Anforderungen für die Verfahren, Prozesse und Leistungsüberwachung, die für die Durchführung und Überwachung der mechanischen Vernichtung von vertraulichen und sensiblen Unterlagen eingeführt werden, um sicherzustellen, dass diese Unterlagen zuverlässig und sicher entsorgt werden.

Dieses Dokument kann von jedem, der solche Unterlagen für sich selbst oder im Auftrag anderer verarbeitet, herangezogen werden und es behandelt die folgenden Szenarien:

- vor Ort – mithilfe mobiler Ausrüstung am Ort der Verwendung (Vernichtungsausrüstung wird zu den vertraulichen und sensiblen Unterlagen gebracht);
- an einem anderen Ort – Transport und anschließende Vernichtung mithilfe von Ausrüstungen in einer Vernichtungsanlage (die vertraulichen und sensiblen Unterlagen werden zur Vernichtungsausrüstung gebracht, wie es in einer von einem Dienstleister betriebenen spezialisierten externen Einrichtung üblich ist);
- mithilfe statischer Ausrüstung am Ort der Verwendung (vertrauliche und sensible Unterlagen sowie Vernichtungsausrüstung befinden sich an einem Ort, wie z. B. ein Schredder in einem von einem oder mehreren Auftraggebern belegten Gebäude).

Vernichtung durch Löschung wird nicht in diesem Dokument behandelt.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 50131-1:2006,¹ *Alarmanlagen — Einbruch- und Überfallmeldeanlagen — Teil 1: Systemanforderungen*

EN 62676-4, *Videoüberwachungsanlagen für Sicherheitsanwendungen — Teil 4: Anwendungsregeln*

ISO/IEC 21964-2:2018, *Information technology — Destruction of data carriers — Part 2: Requirements for equipment for destruction of data carriers*

EN 1627:2021, *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse — Einbruchhemmung — Anforderungen und Klassifizierung*

EN 1628:2021, *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse — Einbruchhemmung — Prüfverfahren für die Ermittlung der Widerstandsfähigkeit unter statischer Belastung*

EN 1629:2021, *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse — Einbruchhemmung — Prüfverfahren für die Ermittlung der Widerstandsfähigkeit unter dynamischer Belastung*

EN 1630:2021, *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse — Einbruchhemmung — Prüfverfahren für die Ermittlung der Widerstandsfähigkeit gegen manuelle Einbruchversuche*

¹ Geändert durch EN 50131-1:2006/A1:2009, EN 50131-1:2006/A2:2017 und EN 50131-1:2006/A3:2020.

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
 - COD = Vernichtungsnachweis (en: certificate of destruction)
 - DSGVO = Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)
 - VSS = Videoüberwachungsanlagen (en: video surveillance systems) (CCTV, en: closed circuit television)
 - RC = niedrige Schutzklasse (en: routine confidential)
 - OS = mittlere Schutzklasse (en: official sensitive)
 - HS = hohe Schutzklasse (en: highly sensitive)
 - ANPR = automatische Nummernschilderkennung (en: automatic number-plate recognition)

3.1

befugte Person

zuverlässige Einzelperson, der in Übereinstimmung mit den Anforderungen ihrer Stelle Zugriff auf vertrauliche und sensible Unterlagen gewährt wird und die entsprechend der angemessenen nationalen Norm sicherheitsüberprüft wurde

3.2

Vernichtungsnachweis

COD, en: certificate of destruction

Bestätigung, dass die auf dem COD aufgeführten vertraulichen und sensiblen Unterlagen den Vernichtungsprozess durchlaufen haben

3.3

Auftraggeber

Eigentümer der vertraulichen oder sensiblen Unterlagen, der ein Unternehmen vertraglich zur Erbringung von Vernichtungsdienstleistungen verpflichtet

3.4

Unternehmen

vom Auftraggeber beauftragte Entität, die als Dienstleister bestimmt ist, die in der Regel auf gewerblicher Basis ein oder mehrere Fähigkeiten anbietet und an die der Auftraggeber eine oder mehrere Aufgaben im Rahmen des Vernichtungsprozesses übertragen hat

3.5

Sachkundiger

Einzelperson mit erforderlichem Wissen oder erforderlicher Fertigkeit, das/die sie über entsprechende Erfahrung, Schulung oder Qualifizierung erworben hat

3.6

vertrauliche Informationen

gespeicherte Fakten oder gespeichertes Wissen, wie medizinische Aufzeichnungen, Finanzunterlagen oder Software-Quellcodes auf Datenträgern, deren Vertraulichkeit der Auftraggeber schützen möchte

3.7

Vertrag

schriftliches Dokument zwischen dem Auftraggeber und dem Unternehmen, das alle Vorgänge abdeckt

3.8

kritischer Lieferant

Auftragnehmer, die Mitarbeiter oder Lieferanten mit Ausrüstung versorgen, die in einem Bereich, einschließlich Fahrzeugen, verwendet werden, in dem vertrauliche oder sensible Unterlagen gelagert oder vernichtet werden dürfen

3.9

Datenbeauftragter

natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die (entweder alleine oder gemeinsam mit anderen Personen) die Verwendungszwecke der Daten und die Art und Weise, in der personenbezogene Daten bearbeitet werden oder bearbeitet werden sollen, festlegt. Eigentümer von personenbezogenen Daten sind Datenbeauftragte

3.10

Datenbearbeiter

natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Daten im Auftrag des Datenbeauftragten verarbeitet. Vernichtungsunternehmen und Dienstleister, die personenbezogene Daten vernichten, sind Datenbearbeiter

3.11

Verformung eines Datenträgers

Prozess, einen Datenträger unlesbar zu machen

Anmerkung 1 zum Begriff: Die Verformung von Unterlagen der Kategorie E in dem Maße, dass die Diskette oder das Medium nicht mehr über ein Lesegerät geführt werden kann, als Datenvernichtung kann bis zu einschließlich Stufe 3 festgelegt werden.

3.12

Vernichtung

Prozess, durch den vertrauliche oder sensible Unterlagen zu Abfall werden

3.13

Ergebnis der Vernichtung

Reduzierung der Größe oder Reduzierung der Zusammensetzung, wodurch die Unterlagen unlesbar, unleserlich, unbrauchbar und nicht rekonstruierbar gemacht werden

3.14

Output der Vernichtung

Unterlagen, die den Vernichtungsprozess durchlaufen haben und zu Abfall werden, wie in diesem Dokument festgelegt

3.15

dokumentiertes Verfahren

aufgezeichnete Beschreibung eines zum Erreichen eines Ziels zu befolgenden Prozesses

3.16

Vernichtungsanlage

Gelände oder mobiles Vernichtungsfahrzeug, wo die Vernichtungsanlage errichtet und betrieben wird

3.17

Lagerstelle

nicht-vernichtende Stelle des Dienstleisters für die sichere Aufbewahrung von zur Vernichtung vorgesehenen, vertraulichen und sensiblen Unterlagen vor dem Transport zur Vernichtungsanlage

3.18

verschlossen

zur Vermeidung von unbefugtem Zugriff physisch gesichert und zur Öffnung geschützte Eingabe, wie eines Schlüssels, eines Tokens oder einer Passphrase, erforderlich

3.19

Art der Unterlagen

Unterscheidung vertraulicher und sensibler Unterlagen nach Informationsdichte und Umfang der Informationen in Kombination mit dem Aufbau des Objekts

3.20

Schutzklasse

Klassifizierung des Schutzbedarfs von vertraulichen und sensiblen Unterlagen

3.21

Aufzeichnung

Dokument in Papier- oder elektronischer Form, das ein Ereignis oder den Abschluss eines Prozesses beschreibt

3.22

versiegelt

mittels einer Durchziehplombe aus Kunststoff, einer Klebplombe oder einem anderem Unversehrtheitssiegel physisch gesichert, um Zugriff auf oder Entnahme von vertraulichen und sensiblen Unterlagen zu verhindern

3.23

gesicherter Bereich

Gebäude, Raum, Empfangsbereich oder Aktenvernichtungsfach eines mobilen Vernichtungsfahrzeugs oder eines Bereichs mit vertraulichen und sensiblen Unterlagen, das/der kontrolliert und vor unbefugtem Zugriff geschützt wird

3.24

Aktenvernichterbeutel

versiegelbarer undurchsichtiger Beutel zur sicheren Aufbewahrung vertraulicher oder sensibler Unterlagen während der Lagerung oder des Transports vor dem Schreddern

3.25

Sicherheitsbehälter

verschießbarer Behälter, z. B. eine Konsole oder eine Tonne, der sicheren Schutz der vertraulichen oder sensiblen Unterlagen einschließlich Datenträger bietet

3.26

Sicherheitsstufe

Klassifizierung des erforderlichen Aufwands, Daten und/oder Informationen wiederzuerlangen oder die ursprüngliche Form von Objekten wiederherzustellen

3.27

sensible Unterlagen

sämtliche Objekte oder Datenträger, die, sofern kompromittiert, nachteilige Auswirkungen auf den Auftraggeber oder eine Einzelperson bzw. Organisation in Verbindung mit dem Objekt hätte. Zu sensiblen Unterlagen zählen Objekte, die vertrauliche Informationen oder sensible Daten (in Papierform, Film, optisch, elektronisch) enthalten, und sonstige Objekte, die sensible Unterlagen (Validierungssiegel, Schlüssel von mechanischen/elektronischen Schlössern, fehlerhafte Produkte, veraltete Markenware) enthalten

3.28

Dienstleister

Organisation oder Einzelperson, einschließlich Unterauftragnehmer, die/der in der Regel auf gewerblicher Basis ein oder mehrere Fähigkeiten im Rahmen des Vernichtungsprozesses anbietet und an die/den der Auftraggeber eine oder mehrere Aufgabe übertragen hat

3.29

Unterauftragnehmer

Dienstleister oder Transportdienstleister, der nicht direkt vom Auftraggeber beschäftigt, aber mit der Ausführung von Arbeiten im Auftrag des Unternehmens beauftragt wird

3.30

Transportdienstleister

Entität, die eine Überbringung vertraulicher oder sensibler Unterlagen zu einer Vernichtungsanlage anbietet

3.31

VSS

Videoüberwachungsanlagen (en: video surveillance systems) – ehemals als CCTV bezeichnet

3.32

Abfall

Output aus dem Vernichtungsprozess, der nicht mehr sensibel oder vertraulich ist, da die Unterlagen die Festlegungen des Auftraggebers hinsichtlich des Outputs der Vernichtung erfüllen

3.33

schriftliche Benachrichtigung

Mitteilung in Papier- oder elektronischer Form, bei der die Zustellung der Nachricht an den Empfänger bestätigt ist; zum Beispiel eine Briefsendung per Einschreiben oder eine E-Mail, für die eine Empfangsbestätigung erhalten wird

4 Schutzklasse

4.1 Allgemeines

Dieses Dokument berücksichtigt, dass Auftraggeber und Datenbeauftragte unterschiedliche Sicherheitsanforderungen und einen unterschiedlichen Schutzbedarf hinsichtlich der Prozesse festlegen, die zu befolgen sind, nachdem vertrauliche oder sensible Unterlagen zur Vernichtung bestimmt werden bis zu dem Punkt, an dem die Unterlagen vernichtet werden.

Der Grad der Sensibilität der Unterlagen bzw. seines Daten- oder Informationsinhalts ermittelt und bestimmt den Bedarf, diese vor einer Verletzung der Grundsätze der Vertraulichkeit, Integrität und Verfügbarkeit zu schützen, und berücksichtigt dabei den Schaden, der aus dieser Verletzung entstehen würde.

Es wird in drei Schutzklassen unterschieden:

- routine confidential (RC) – routinemäßig vertraulich: erfordert normale Schutzmaßnahmen;
- official sensitive (OS) – offiziell sensibel: erfordert erhöhte Schutzmaßnahmen;
- highly sensitive (HS) – hochsensibel: erfordert sehr hohe Schutzmaßnahmen.

4.2 Bestimmung der Schutzklasse

Damit die Datenträgervernichtung mit den Grundsätzen der Wirtschaftlichkeit und Verhältnismäßigkeit vereinbar ist, müssen die darauf enthaltenen Daten einer Schutzklasse zugewiesen werden. Die Sicherheitsstufe, die für die Datenträgervernichtung gewählt wird, wird von der Schutzstufe der Daten bestimmt.

Schutzklasse RC, übliche Schutzstufe für interne Daten:

- die häufigste Einstufung von Informationen, für große Personengruppen bestimmt;
- eine unbefugte Weitergabe oder Veröffentlichung würde eingeschränkte negative Auswirkungen auf die Organisation haben;
- der Schutz von personenbezogenen Daten muss sichergestellt werden. Andernfalls besteht das Risiko, dass betroffene Personen in ihrem Ansehen oder ihrer wirtschaftlichen Lage Schaden erleiden.

Schutzklasse OS,

höhere Schutzstufe für vertrauliche Daten:

- die Informationen sind auf eine kleine Personengruppe begrenzt;
- eine unbefugte Weitergabe würde schwerwiegende Auswirkungen auf die Organisation haben und kann unter Umständen eine Verletzung von Gesetzen oder vertraglichen Verpflichtungen mit sich bringen;
- der Schutz von personenbezogenen Daten muss hohen Anforderungen entsprechen. Andernfalls besteht das Risiko, dass betroffene Personen in ihrer gesellschaftlichen Stellung oder ihrer wirtschaftlichen Lage großen Schaden erleiden.

Schutzklasse HS,

sehr hohe Schutzstufe für streng vertrauliche und geheime Daten:

- die Informationen sind auf eine sehr kleine Personengruppe begrenzt, deren Mitglieder namentlich bekannt und zum Zugriff befugt sind;
- eine unbefugte Weitergabe würde schwerwiegende (existenzbedrohende) Auswirkungen auf die Organisation haben und/oder würde eine Verletzung von Berufsgeheimnissen, Verträgen und Gesetzen mit sich bringen;
- der Schutz von personenbezogenen Daten muss strikt sichergestellt werden. Andernfalls können das Leben und die Sicherheit der betroffenen Personen oder ihre persönliche Freiheit gefährdet sein.

5 Bestimmung der Sicherheitsstufe

5.1 Allgemeines

Es muss ein Maß für die Vernichtung bestimmt werden, indem ein Ergebnis gewählt wird, dessen Abfall nicht mehr vertraulich oder sensibel ist.

Unter Berücksichtigung des Stands der Technik, der Kosten für die Umsetzung und der Art, des Umfangs, des Rahmens und der Zwecke der Verarbeitung sowie des Risikos einer unterschiedlich großen Wahrscheinlichkeit und eines anderen Schweregrads der Sicherheitsverletzung müssen der Auftraggeber als Datenbeauftragter und das Unternehmen/der Dienstleister als Datenbearbeiter angemessene technische und organisatorische Maßnahmen und ein Vernichtungsverfahren einführen und beschließen, um eine dem Risiko angemessene Sicherheitsstufe sicherzustellen, einschließlich der Sicherstellung der fortlaufenden Vertraulichkeit, Integrität und Widerstandsfähigkeit der Verarbeitungssysteme und -dienste, bis die Unterlagen zum erforderlichen Ergebnis der Vernichtung vernichtet sind (DSGVO, Artikel 32, Eins (b)), so dass sichergestellt ist, dass sie nicht leserlich, lesbar, brauchbar und rekonstruierbar sind.

Passend zur Schutzklasse muss eine Sicherheitsstufe von 1 bis 7 und ein Vernichtungsverfahren gewählt werden, die für das Ergebnis der Vernichtung sorgen, das vom Auftraggeber als angemessen für vertrauliche und sensible Unterlagen nach Abschluss der Vernichtung beschlossen wurde. Siehe nachstehende Tabelle 2.

Tabelle 2 — Zuweisung der Sicherheitsstufe und Schutzklassen

Schutzklasse	Sicherheitsstufen						
	1	2	3	4	5	6	7
RC	x ^a	x ^a	x				
OS			x	x	x		
HS				x	x	x	x
^a Diese Kombination kann nicht für personenbezogene Daten verwendet werden.							

6 Erhöhung der Sicherheitsstufe

6.1 Allgemeines

Ausschließlich bei einem Ergebnis der Vernichtung in der Kategorie P und Kategorie F und bei Unterlagen, die nach Sicherheitsstufe 1, 2 oder 3 vernichtet wurden, kann unter Umständen ein Mischen und Verdichten die Sicherheit nur einmal auf die nächsthöhere Stufe erhöhen, bis maximal Sicherheitsstufe 4, vorausgesetzt die folgenden Kriterien sind erfüllt:

- das Mischen umfasst mindestens 100 kg jeder einzelnen Art der Unterlagen der Kategorie P, die als die Gesamtmasse der Partikel und Fragmente innerhalb des vernichteten Outputs darzustellen sind und die in einem einzelnen unterbrechungsfreien Zyklus der Maschine oder Ausrüstung zu vernichten sind;
- das Unternehmen/der Dienstleister erhält vom Auftraggeber eine explizite Bestätigung, dass die Verfahren zur Erhöhung der Sicherheitsstufe für diese spezifische Arbeitsanweisung angewendet werden dürfen.

Mischen und Verdichten von Unterlagen, die auf der Sicherheitsstufe 1 und der Sicherheitsstufe 2 vernichtet wurden, dürfen nicht als Mittel zur Erhöhung der Sicherheitsstufe bei der Vernichtung von als Unterlagen der Kategorie P eingestuften personenbezogenen Daten verwendet werden.

Es wird empfohlen, dass der Auftraggeber oder Datenbeauftragte der Unterlagen die Lagerung des Outputs der Vernichtung in Betrachtung zieht, sobald dieser zu Abfall wurde. Ein Dokument in Papier ist einfacher wiederherzustellen, wenn alle seine Einzelteile an einem Ort aufbewahrt werden. Es ist bekannt, dass das Mischen und Verdichten des Outputs der Vernichtung in größeren Mengen und aus mehreren Quellen zu einer Zerstreuung des Abfalls führt und eine Wiederherstellung unwahrscheinlicher machen kann. Die hat keine Auswirkung auf den möglichen Informationsinhalt der einzelnen Partikel der Unterlagen.

Bei der Auswahl der angemessenen Sicherheitsstufe müssen die Dichte und/oder Größe der auf dem Datenträger dargestellten Informationen berücksichtigt werden. Falls aufgrund der Farbe oder anderer Merkmale des Datenträgers die Wiederherstellung einfacher ist, muss möglicherweise eine höhere Sicherheitsstufe gewählt werden.

7 Vernichtungsausrüstung

7.1 Allgemeines

Die folgenden Anforderungen gelten für alle Ausrüstungen zur mechanischen Vernichtung und die zugehörigen Verfahren. Sie gelten an jedem Ort: am Standort des Auftraggebers, in einem mobilen Fahrzeug oder in einer Vernichtungsanlage.

7.2 Verwendung von Vernichtungsausrüstung

Vernichtungsausrüstung muss von befugten, angemessen geschulten Mitarbeitern bedient werden oder die Bedienung wird von befugten Mitarbeitern in Übereinstimmung mit Abschnitt 9, Kontrolle des Zugriffs, überwacht.

Das Bedienpersonal darf keinen Zugriff auf nicht geschredderte Datenträger mit Abbildung in Originalgröße haben. Die für die Datenträgervernichtung verwendete Maschine wird bespeist, indem der Inhalt der Sicherheitsbehälter entweder direkt oder von einer entsprechend gesicherten Zuführvorrichtung in die Maschine oder Fülltrichter gegeben wird. Die Anforderung, dass die Ausrüstung grundlegend zugriffssicher (en: „fundamentally access-proof“) sein muss, ist so zu verstehen, dass JEDER Zugriff sowohl im gewöhnlichen Vernichtungsprozess als auch aufgrund der Konstruktionsmerkmale der betreffenden Anlage, physisch verboten ist. Aus diesem Grund ist der Transfer von Datenträgern (z. B. aus großvolumigen Behältern) in einen Sammeltrichter oder Bunker sowie die Möglichkeit der Handsortierung nicht ausreichend, um die Anforderungen der Schutzklasse HS zu erfüllen. Der Grund dafür sind die wesentlichen Konstruktionsgrundsätze, die dazu führen können, dass Datenträger während des regulären Prozesses im offenen Bereich zurückbleiben und manuell entfernt werden müssen. Jegliche Abweichung ist nur im Falle von technischen Störungen am Vernichtungsmotor selbst oder am Hebe-/Transfermechanismus des Behälters zulässig (z. B. im Brandfall).

Im Falle, dass Unterlagen unterschiedlicher Schutzklassen oder Sicherheitsstufen vermischt werden, müssen alle Unterlagen nach der höchsten, in der Lieferung erforderlichen Sicherheitsstufe vernichtet werden.

7.3 Bedienungsanleitung

Anleitungen, die den Bediener befähigen, das Ergebnis der Vernichtung zu erhalten, müssen auf dem Gelände des Dienstleisters der Vernichtung zur Verfügung stehen.

Der Bereich der von der Vernichtungsausrüstung erzielbaren Sicherheitsstufen muss schriftlich festgehalten sein und den Bedienern der Maschine und für die Prüfung zur Verfügung stehen.

7.4 Ergebnis der Vernichtung

Der Output der Unterlagen aus der Vernichtungsausrüstung muss stichprobenartig geprüft werden, um sicherzustellen, dass die Ausrüstung vertrauliche und sensible Unterlagen vernichten kann und Abfall in Übereinstimmung mit den in Anhang A, Ergebnisse der Vernichtung, aufgeführten Ergebnissen der Vernichtung erzeugt.

7.5 Bestätigung des Vernichtungsprozesses und dessen Abschluss

Sobald die Vernichtung abgeschlossen ist, darf eine befugte Person durch Sichtprüfung bestätigen, dass alle vertraulichen und sensiblen Unterlagen, die dem Vernichtungsprozess der Ausrüstung zugeführt wurden, vernichtet wurden und dass der Prozess das erforderliche Ergebnis erzielt hat.

Das Unternehmen muss durch Untersuchen der Output-Unterlagen sicherstellen, dass die Vernichtung einer Lieferung abgeschlossen ist.

Das Unternehmen muss bestätigen, dass der Auftraggeber berechtigt ist, die Vernichtung seiner Unterlagen zu überwachen.

Der Auftraggeber ist berechtigt, eine Probe der vernichteten, vertraulichen und sensiblen Unterlagen zu nehmen.

7.6 Wartung und Leistungsüberwachung

Die Vernichtungsausrüstung muss wie folgt regelmäßig kontrolliert und gewartet werden:

- die Leistung der Ausrüstung muss überwacht werden, um sicherzustellen, dass der Output dem Ergebnis der Vernichtung wie in Anhang A (Ergebnisse der Vernichtung) aufgeführt entspricht;
- die Leistung der Ausrüstung, einschließlich der austauschbaren Module, Siebe oder Messer, muss von einem Sachkundigen bewertet werden, um sicherzustellen, dass der erzielte Output dem schriftlich festgelegten Output der Vernichtung entspricht;
- die Ausrüstung muss vor dem ersten Gebrauch und anschließend regelmäßig von einem Sachkundigen bewertet werden. Die Häufigkeit der Bewertungen ist in nachstehend in 7.7 aufgeführt;
- nach Montage, Wartung oder Modifizierung muss die Intaktheit der Ausrüstung von einer befugten Person bestätigt werden, um sicherzustellen, dass die Ausrüstung nicht derart modifiziert wurde, dass eine vorsätzliche Sicherheitsverletzung erleichtert wird;
- Prüfungen und Bewertungen müssen dokumentiert werden und sollten mindestens die Punkte in Tabelle 3 enthalten. In der Aufzeichnung muss der Grund für die Prüfung oder Bewertung genannt werden.

Falls die Leistung der Ausrüstung nicht dem Ergebnis der Vernichtung entspricht, muss eine Korrekturmaßnahme ergriffen werden und eine weitere dokumentierte Prüfung erfolgen, bevor die Ausrüstung für die sichere Vernichtung vertraulicher und sensibler Unterlagen verwendet werden kann.

Tabelle 3 — Aufzeichnung der Prüfung und Bewertung der Vernichtungsausrüstung

- | |
|---|
| <ul style="list-style-type: none">• Angabe der Seriennummer der Ausrüstung• Grund für Prüfung/Bewertung• Datum und Uhrzeit der Prüfung• Name und Organisation der Person(en), die die Prüfung durchführt/durchführen• Beschreibung des geprüften Outputs• Bestätigung der Konformität oder Angaben zu den ergriffenen Korrekturmaßnahmen |
|---|

7.7 Häufigkeit der Bewertung von Vernichtungsausrüstung

Das Unternehmen muss die Wartung als Mindestanforderung wie vom Hersteller vorgeschrieben und/oder empfohlen in den vom Hersteller festgelegten Zeitintervallen durchführen.

Das spezifische Intervall für die Wartung von Verschleißteilen, die die erreichte Qualität der Vernichtung beeinflussen können (z. B. Schneidvorrichtung, Messer, Klingen, Gegenmesser, perforierte Sortiersiebe), hängt vom Maschinentyp sowie von der Art und Dauer des Maschineneinsatzes ab (Kategorie der Unterlagen, Vernichtungsvolumen).

Bediener der Vernichtungsausrüstung oder Sachkundige müssen in einem Abstand von mindestens einer Woche eine Sichtprüfung der Maschinen durchführen, um zu bestätigen, dass alles einwandfrei funktioniert, um das erforderliche Ergebnis der Vernichtung zu erzielen.

Bediener der Ausrüstung sollten regelmäßig während der gesamten Betriebsdauer der Maschine oder Ausrüstung die Partikelgröße prüfen, da Verschleiß oder Beschädigung der Schneidmesser die Leistungsfähigkeit hinsichtlich des Ergebnisses in der Partikelgröße verringern kann.

Das Unternehmen ist für die Ermittlung der angemessenen Wartungsintervalle verantwortlich oder gibt fachliche Schätzungen oder Wartungsdienstvereinbarungen mit der gebotenen Sorgfalt und muss diese dem Auftraggeber auf Anfrage zur Verfügung stellen.

Die Vernichtungsausrüstung muss in Übereinstimmung mit ISO/IEC 21964-2:2018, Abschnitt 5, Abschnitt 6 und Abschnitt 7, von einem Vertreter des Herstellers oder einem Sachkundigen nach der Montage und anschließend alle fünf Jahre bewertet werden, um zu prüfen, ob die Maschine weiterhin gebrauchstauglich ist und die zertifizierten Ergebnisse erzielt werden. Nach erfolgreicher Prüfung muss ein Fünf-Jahres-Zertifikat ausgestellt werden. Im Falle einer erfolglosen Prüfung sollte die Vernichtungsausrüstung so lange nicht verwendet werden, bis eine weitere Prüfung bestätigt, dass die Maschinen korrigiert wurden, damit sie die erforderlichen Ergebnisse erzielen, und bis ein neues Konformitätszertifikat ausgestellt wurde.

7.8 Redundanz von Vernichtungsausrüstung

Die Redundanz und Verfügbarkeit der Maschine für die Vernichtung von Unterlagen müssen durch einen Notfallplan sichergestellt werden. Bei einer nicht vor Ort auf dem Gelände erfolgenden Vernichtung besteht kein Bedarf an einer zweiten verfügbaren Maschine, aber es muss sichergestellt werden, dass die Vernichtung abgeschlossen wird, um die Fristenvorgabe zu erfüllen.

Die Verfügbarkeit der Vernichtungsmaschine muss durch einen Notfallplan sichergestellt werden, der für Schutzklasse OS und Schutzklasse HS erforderlich und für Schutzklasse RC möglich ist.

8 Gelände des Unternehmens für die Vernichtung und Lagerstellen des Dienstleisters

Das Gelände des Unternehmens für die Vernichtung und die Lagerstellen des Dienstleisters müssen entsprechend der nach Anhang B bestimmten Schutzklasse über Schutz- und Sicherheitsmaßnahmen verfügen. Das Unternehmen muss eine verschließbare Verwaltungsstelle und ein betriebliches Zentrum haben, wo Belege, geschäftliche Dokumente, Zertifikate, Schriftverkehr, Akten usw., die für die Ausführung der Geschäftsvorgänge erforderlich sind, aufbewahrt werden.

Alle physischen Sicherheitsmaßnahmen und Verfahrenskontrollen müssen für den Risikograd im Zusammenhang mit den vertraulichen und sensiblen Unterlagen angemessen sein, um einen Angriff oder Verlust zu vermeiden.

Die Lagerstellen des Dienstleisters dürfen nicht für vertrauliche und sensible Unterlagen der Schutzklasse HS genutzt werden. Die Lagerstellen müssen mit Sicherheitsverfahren geschützt werden, die zur Sensibilität der Unterlagen verhältnismäßig sind. Die Unterlagen dürfen nicht länger als 24 h an der Lagerstelle aufbewahrt werden.

Ein gesicherter Bereich muss geschützt werden, solange sich dort vertrauliche und sensible Unterlagen befinden. Dazu würden neben Lagerstellen auch das Gelände für die Vernichtungsanlage des Unternehmens zählen. Vertrauliche und sensible Unterlagen müssen mit Maßnahmen geschützt werden, die mit der bestimmten Schutzklasse und den spezifischen Anforderungen des Auftraggebers in Übereinstimmung stehen.

8.1 Gesicherte Bereiche auf dem Gelände für die Vernichtung und in den Lagerstellen des Dienstleisters

Der gesicherte Bereich muss in massiver Bauweise (z. B. durch Stahlbeton, massives Mauerwerk oder Gleichwertiges) unter Berücksichtigung der erforderlichen Schutzelemente, um die Risikotoleranz hinsichtlich der Schutzklassen zu erfüllen, errichtet sein.

Ein Gelände für die Vernichtung und die Lagerstellen des Dienstleisters müssen physisch von anderen Organisationen durch eine Massivwand isoliert sein.

Wenn der gesicherte Bereich ein kleinerer Bereich innerhalb der gesamten Vernichtungsanlage oder der gesamten Lagerstelle des Dienstleisters ist, müssen die gesicherten Bereiche als geschlossener Bereich ausgelegt sein, der ausschließlich zum Zwecke der Vernichtung vertraulicher und sensibler Unterlagen genutzt wird und physisch von anderen Geschäftsaktivitäten auf demselben Gelände abgetrennt ist. Gesicherte Bereiche müssen so ausgelegt sein, dass sie vor Angriff und unbefugtem Zutritt schützen.

Was mobile Schredderfahrzeuge betrifft, ist die Anforderung eines sicheren Bereichs dann gegeben, wenn die Schredderanlage nicht betretbar ist.

8.2 Sicherheit

Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse, die den Zutritt zu Verarbeitungs-, gesicherten und Bürobereichen ermöglichen, müssen über eine hohe physische Sicherheit verfügen und müssen mit geeigneten Schlössern ausgestattet sein, die mindestens EN 1627:2021, EN 1628:2021, EN 1629:2021 und EN 1630:2021 oder äquivalenten nationalen Normen, maßgebenden behördlichen Anforderungen oder vertraglichen Versicherungsanforderungen entsprechen. Das in diesen Normen oder Anforderungen festgelegte Schutzniveau sollte durch Risikobeurteilungen des Unternehmens in Verbindung mit der Schutzklasse und den Anforderungen des Auftraggebers bestimmt werden.

In den Geschäftsräumen muss eine Einbruchmeldeanlage nach EN 50131-1:2008¹ mit Überwachung durch eine Alarmempfangszentrale installiert sein. Die Anlage muss als Mindestanforderung die Verarbeitungs-, gesicherten und Bürobereiche schützen.

Falls entweder die geeigneten Schlösser oder eine Einbruchmeldeanlage aufgrund einer Störung oder Wartung nicht funktioniert, muss das Gelände, wenn unbeaufsichtigt, bewacht werden, sofern dort vertrauliche oder sensible Unterlagen gelagert werden.

Ein Videoüberwachungssystem (auch als CCTV bezeichnet) mit Aufzeichnungseinrichtung nach EN 62676-4 muss installiert sein, um die Eingänge zu den gesicherten Bereichen, die Entlade-, gesicherten und Verarbeitungsgebiete zu überwachen. Dies muss immer dann gelten, wenn das Schreddern in gewerblichem Umfang erfolgt, unabhängig davon, wer Eigentümer des Standorts ist bzw. diesen kontrolliert.

Eine Risikobeurteilung des Unternehmens sollte durchgeführt werden, um festzustellen, ob weitere Schutzmaßnahmen erforderlich sind.

Schutzmaßnahmen zur physischen Sicherheit müssen einzelnen Risikobeurteilungen unterzogen werden, müssen aber mindestens Folgendes enthalten:

Bei Schutzklasse RC und Schutzklasse OS:

- alle Türen und Tore, die direkt zu einem gesicherten Bereich führen, schließen automatisch oder es wird mit einem optischen oder akustischen Signal auf offene Türen und Tore hingewiesen;
- die Bewegung jedes Fahrzeugs Dritter auf dem Unternehmensgelände muss strengstens kontrolliert werden.

Bei Schutzklasse HS:

- wenn Türen und Tore, die direkt zu einem gesicherten Bereich führen, länger als gewöhnlich offen stehen, wird automatisch eine Nachricht an den Sicherheitsbeauftragten vor Ort gesendet;
- eine überwachte Einbruchmeldeanlage spezifisch für die Zone des gesicherten Bereichs wird eingestellt, wenn der gesicherte Bereich unbeaufsichtigt ist.

9 Kontrolle des Zugriffs

9.1 Allgemeines

Der Zugang zu einem gesicherten Bereich, der vertrauliche und sensible Unterlagen enthält, muss kontrolliert werden.

Das Unternehmen ist verpflichtet, dem Kunden Zugang zu verschaffen, damit er Zugriff auf seine eigenen vertraulichen oder sensiblen Unterlagen haben oder diese einsehen kann.

Das Unternehmen muss über ausreichende und angemessene Schutzeinrichtungen in Bezug auf die Schutzklasse verfügen, um den Zugriff eines besuchenden Auftraggebers auf die vertraulichen oder sensiblen Unterlagen eines anderen Auftraggebers zu verhindern.

Alle Personen, denen Zugriff auf vertrauliche Informationen, Datenträger und sensible Unterlagen oder Zugang zu gesicherten Bereichen, in denen möglicherweise vertrauliche oder sensible Objekte und/oder Vernichtungsausrüstung zur Vernichtung dieser Unterlagen aufbewahrt werden, gewährt wird, müssen das in 9.2 dargelegte Verfahren befolgen und müssen

- a) Mitarbeiter des Unternehmens, die zum Zugriff auf die entsprechende Schutzklasse befugt sind, oder
- b) Mitarbeiter des Unternehmens, die in dem mit dem Auftraggeber vereinbarten Maß sicherheitsüberprüft sind, oder
- c) Mitarbeiter des Auftraggebers oder Besucher des Auftraggebers sein, denen vom jeweiligen Auftraggeber Zugriff gewährt wurde.

Zusätzlich zu den vorgenannten Maßnahmen und von ihnen unabhängig darf der Zugriff auf oder die Sichtprüfung von Unterlagen der Schutzklasse HS nicht erlaubt oder ermöglicht werden.

9.2 Autorisierung des Zugriffs von Unternehmensmitarbeitern

Alle Mitarbeiter des Unternehmens mit Zugang zu einem gesicherten Bereich oder Zugriff auf vertrauliche und sensible Unterlagen sollten für die angemessene Berechtigungsstufe der vertraulichen und sensiblen Unterlagen sicherheitsüberprüft sein, sofern dies vom Auftraggeber gefordert wird.

Das Unternehmen muss über ein dokumentiertes Verfahren zur Autorisierung der Mitarbeiter verfügen. Aufzeichnungen der befugten Personen müssen mindestens Folgendes enthalten:

- Name der Person und Zugriffsstatus der Sicherheitsstufe;
- Datum der Autorisierung;
- Name und Stelle im Unternehmen der Person, die die Autorisierung gewährt.

Es wird empfohlen, die Autorisierung regelmäßig zu überprüfen.

Es wird empfohlen, dass die Zugriffskontrollsysteme spezifisch für Personen sind, die eine bestimmte Tätigkeit ausüben, und müssen entweder ermessensfrei, verpflichtend oder rollenbasiert sein.

9.3 Begleiteter Zugriff für Unternehmensmitarbeiter ohne entsprechende Schulung

Das Unternehmen darf entscheiden, Mitarbeitern des Unternehmens den Zugang zu einem gesicherten Bereich zu gewähren, die keine entsprechende Schulung entsprechend des Verfahrens des Unternehmens abgeschlossen haben, unter der Voraussetzung, dass die folgenden Kriterien erfüllt sind:

- eine angemessene Sicherheitsüberprüfung wurde wie in 13.2 beschrieben zufriedenstellend durchgeführt und die Mitarbeiter haben eine Vertraulichkeitsvereinbarung unterzeichnet;
- eine Person, der Zugang zu einem gesicherten Bereich gewährt wird, die aber nicht geschult ist, muss je nach Schutzklasse wie in nachstehender Tabelle 4 festgelegt von einer oder mehreren zugewiesenen befugten Personen begleitet und beobachtet werden.

9.4 Zugang zu gesichertem Bereich für Besucher und Auftragnehmer

Mitarbeiter des Unternehmens müssen alle Besucher begleiten, solange diese sich in unternehmenseigenen Räumlichkeiten, gesicherten Bereichen und Fahrzeugen zur Abholung des Unternehmens aufhalten.

Alle Besucher und Auftragnehmer, die temporären Zugang zu gesicherten Bereichen anfordern, müssen vom Unternehmen verifiziert und autorisiert werden, bevor sie Zugang zu einem gesicherten Bereich erhalten.

Alle Besucher und Mitarbeiter des Auftragnehmers müssen eine Vertraulichkeitsvereinbarung vor dem Zugang abschließen. Der Besucher stimmt zu, dass er die vertraulichen oder sensiblen Unterlagen nicht verwendet, verbreitet, vervielfältigt, offenlegt, verkauft oder anderweitig an andere weitergibt, sofern nicht vom Unternehmen gestattet. Es muss klargestellt werden, dass ein Besucher Informationen über offengelegte Mängel und/oder Schwächen an befugte Dritte soweit zumutbar nur in dem Maß, das für die Erfüllung ihrer Verpflichtungen unbedingt erforderlich ist, weitergeben darf.

9.5 Durchführung der Kontrolle des Zugriffs

Es muss ein Prozess auf Grundlage der Risikobeurteilung des Unternehmens in Bezug auf die Schutzklasse eingerichtet werden.

Es wird empfohlen, dass die Durchführung vor der Gewährung des Zugangs zu gesicherten Bereichen erfolgt:

- a) die Anfrage auf Zugang eines Besuchers oder Auftragnehmers zu einem gesicherten Bereich muss mit dem Anfragsteller oder Gastgeber des Unternehmens, wie zutreffend, geprüft werden;
- b) der Status der Sicherheitsüberprüfung des Besuchers oder der Mitarbeiter des Auftragnehmers, die den Zugang anfordern, muss bestätigt werden;
- c) der Besucher oder die Mitarbeiter des Auftragnehmers müssen über die in den gesicherten Bereichen geltenden Regeln aufgeklärt werden. Während seines Besuchs ist es dem Besucher nicht gestattet jegliche Dokumente, Unterlagen und Ausrüstung, die als vertrauliche oder sensible Unterlagen definiert sind, zu fotografieren, aufzuzeichnen oder zu entfernen, sofern nicht vom Unternehmen dazu gestattet;
- d) beim Betreten wie auch beim Verlassen der Vernichtungsanlage müssen alle Besucher und Mitarbeiter des Auftragnehmers sich mit ihrer Unterschrift an- bzw. abmelden;
- e) allen Besuchern muss ein(e) Ausweisdokument/-karte ausgestellt werden.

9.6 Anforderungen an die Zugriffsstufe

Besucher oder Mitarbeiter des Auftragnehmers, denen Zugang zu einem gesicherten Bereich gewährt wird, müssen je nach Schutzklasse wie in nachstehender Tabelle 4 festgelegt von einer oder mehreren zugewiesenen befugten Personen begleitet und beobachtet werden.

Tabelle 4 — Zugriffsstufe

Schutzklasse	Zu begleitende Personen ohne Autorisierung	Mindestanzahl an befugten Personen, die begleiten
Schutzklasse RC	2	1
Schutzklasse OS	2	1
Schutzklasse HS	1 oder 2 (auftraggeberspezifisch)	1

Aufzeichnungen aller Besucher und Mitarbeiter des Auftragnehmers, denen Zugang erteilt wurde, müssen aufbewahrt werden und mindestens folgende Angaben enthalten:

- Name der Person und vertretene Organisation;
- Status der Sicherheitsüberprüfung der Person;
- Name und Status des Gastgebers des Unternehmens oder Anfragestellers des Auftraggebers;
- Datum und Uhrzeit des Zugangs und des Verlassens;
- Name und Stelle im Unternehmen der Person, die Zugang gewährt;
- Name und Stelle im Unternehmen der befugten Person, die die Person begleitet.

ANMERKUNG Beispiele für Anfragen von Personen, denen Zugang zu einem gesicherten Bereich erteilt werden soll, sind Besucher der Vernichtungsanlage, Vertreter des Auftraggebers oder Wartungsunternehmen, die im Auftrag des Unternehmens arbeiten.

10 Vertrag

10.1 Allgemeines

Es wird empfohlen, dass das Unternehmen vom Auftraggeber vollständig über das mögliche Risiko aufgeklärt wird, damit eine Zusicherung gegeben werden kann.

Mit dem Auftraggeber müssen spezifische Maßnahmen vereinbart werden, um sicherzustellen, dass geeignete Schutzmaßnahmen und physische Sicherheit eingerichtet sind, um mit den festgestellten Sicherheitsrisiken in Bezug auf jede Phase des gesamten Prozesses umzugehen. Der Mindestumfang eines Kriteriums hinsichtlich jeder Schutzklasse ist in der Tabelle mit Kriterien zum sicheren Vernichtungsprozess in Anhang B aufgeführt.

Es muss ein schriftlicher Vertrag, der die Art und den Zweck der Unterlagenverarbeitung, die Sicherheitsstufe und die Schutzklasse zusammen mit den vereinbarten Verantwortlichkeiten seitens des Dienstleisters regelt, zwischen dem Auftraggeber und dem Unternehmen, das als Dienstleister agiert, bestehen.

Der Vertrag muss Informationen enthalten, die bestätigen, dass der Dienstleister

- diese Norm/Verfahrensregeln erfüllt,
- über angemessene, mit dem Auftraggeber vereinbarte Sicherheits- und Schutzmaßnahmen verfügt,

- die erforderlichen Lizenzen besitzt und die geltenden Verordnungen für die Handhabung und den Transport von vertraulichen und sensiblen Unterlagen, einschließlich lokale Abfallverordnungen, einhält,
- die Versicherungen, wie sie im Land des Einsatzes vorgeschrieben sind, abgeschlossen hat und
- über eine Berufshaftpflichtversicherung für die erbrachte Dienstleistung verfügt.

Fristen für den Abschluss des Vernichtungsprozesses sind in 15.1 und in Anhang B festgelegt.

Der Vertrag enthält eine Anforderung an den Auftraggeber, dass er sich dazu verpflichtet

- einen Dienstleister auszuwählen, der genügend Sicherheit hinsichtlich der technischen und organisatorischen Sicherheits- und Schutzmaßnahmen gewährleistet, die für die durchzuführende Bearbeitung bestimmend sind, und
- angemessene Schritte zu unternehmen, um die Einhaltung dieser Maßnahmen und Verfahrensregeln sicherzustellen.

11 Aufzeichnung des Sammelprozesses bis zur Vernichtung

11.1 Allgemeines

- Zum Zeitpunkt der Übergabe muss eine Aufzeichnung der Übergabe der vertraulichen und sensiblen Unterlagen vom Auftraggeber an einen Dienstleister oder einen Transportdienstleister geführt werden.
- Die Aufzeichnung der nachfolgenden Übergabe der vertraulichen und sensiblen Unterlagen vor und einschließlich der Vernichtungsanlage muss deutlich die Überwachungskette zeigen.
- Diese Aufzeichnungen müssen folgende Angaben enthalten:

11.1.1 Aufzeichnung der Übergabe von vertraulichen und sensiblen Unterlagen

In der Aufzeichnung der Übergabe von vertraulichen und sensiblen Unterlagen müssen mindestens die folgenden Angaben enthalten sein:

- a) aktueller Inhaber der vertraulichen und sensiblen Unterlagen (Name des Übergebers, d. h. Name und Anschrift des Auftraggebers sowie SIC-Code);
- b) Sammler der vertraulichen und sensiblen Unterlagen (Name des Empfängers, d. h. Name und Anschrift des Unternehmens sowie Angabe der Lizenz);
- c) wo (Anschrift der Sammlung oder Übergabe);
- d) wann (Datum und Zeitpunkt der Sammlung oder Übergabe);
- e) was (Schutzklasse, Sicherheitsstufe und Unterkategorien der vertraulichen oder sensiblen Unterlagen);
- f) wie (wie werden die vertraulichen oder sensiblen Unterlagen aufbewahrt, möglicherweise die Art des Behälters);
- g) wie viel (Menge der vertraulichen oder sensiblen Unterlagen oder Anzahl und Art der Behälter und/oder Gewicht);
- h) Europäischer Abfallkatalog (EAK) aus Liste der Abfallverordnungen (sofern zutreffend);

- i) Befugnisnachweis zur Durchführung der Arbeit (Unterschrift des Auftraggeber oder Übergebers);
- j) Unterschrift des Empfängers (Unternehmen oder Transportdienstleister), die den Erhalt der vertraulichen und sensiblen Unterlagen und die Übernahme der Verantwortung für die Erbringung der Dienstleistung bestätigt.

Diese Informationen bestimmen die Übergabe der Verwahrung und des Risikos von einer Entität an eine andere.

ANMERKUNG Hinsichtlich der Beförderung und des Transfers von Abfallmaterial und der erforderlichen Aufzeichnungen gelten möglicherweise nationale Gesetze.

11.1.2 Vernichtungsnachweis

Der Abschluss der Vernichtung von vertraulichen und sensiblen Unterlagen muss aufgezeichnet werden.

Es ist eine Bestätigung der Vernichtung für den Auftraggeber durch Ausstellen eines Vernichtungsnachweises erforderlich.

In der Aufzeichnung des Vernichtungsnachweises müssen mindestens die folgenden Angaben enthalten sein:

- a) Name des Dienstleisters;
- b) Name des Auftraggebers;
- c) Kategorie der Unterlagenart (vertrauliche oder sensible Unterlagen);
- d) wie viel (Menge der Behälter, eventuell Gewicht);
- e) wann Vernichtung abgeschlossen (Datum und Uhrzeit);
- f) wo (Ort der Vernichtung);
- g) geltende Sicherheitsstufe und Schutzklasse.

ANMERKUNG Die Aufzeichnung der Unterlagenübergabe und die Aufzeichnung des Vernichtungsnachweises können das gleiche Dokument darstellen, vorausgesetzt, alle relevanten Kriterien sind erfüllt.

12 Unterauftragsvergabe

12.1 Allgemeines

Arbeit darf nur an einen unterauftragnehmenden Dienstleister vergeben werden, der dieses Dokument berücksichtigt.

Der Auftraggeber muss im Voraus informiert werden und muss den Einsatz eines Unterauftragnehmers zur sicheren Vernichtung oder zum Transport vertraulicher und sensibler Unterlagen genehmigen.

Das Unternehmen/der Dienstleister muss dem Auftraggeber den Namen, die Anschrift und die von jedem Unterauftragnehmer erbrachte Dienstleistung mitteilen und muss auf Anfrage dem Auftraggeber alle seine vertraglichen Vereinbarungen mit dem Unterauftragnehmer zum Datenschutz bereitstellen.

Unterauftragnehmer müssen über alle geltenden vom Auftraggeber geforderten Schutzmaßnahmen in Kenntnis gesetzt werden.

13 Mitarbeiter des Unternehmens

13.1 Vertraulichkeitsvereinbarung

Alle Mitarbeiter des Unternehmens mit Zugriff auf vertrauliche und sensible Unterlagen, einschließlich mit Verwaltungsaufgaben, müssen eine Vertraulichkeitsvereinbarung unterzeichnen, die das Unternehmen vor der Beschäftigung, die den Umgang mit vertraulichen und sensiblen Unterlagen beinhaltet, aushändigt.

Durch Unterzeichnen einer Vertraulichkeitsvereinbarung muss der Mitarbeiter zustimmen, dass er während seiner Beschäftigung und nach seiner Anstellung beim Unternehmen keine vertraulichen oder sensiblen Unterlagen offenlegt, mit denen er während seiner Beschäftigung in Kontakt kommt.

Vorbehaltlich der Anforderung des Auftraggebers oder der Maßnahmen aus der Risikobeurteilung einer Schutzklasse müssen die Mitarbeiter des Unternehmens eventuell eine angemessene rechtliche Verschwiegenheitspflicht übernehmen.

13.2 Sicherheitsüberprüfung der Mitarbeiter

Alle Mitarbeiter, die vom Unternehmen zur Verwaltung, Sammlung und Vernichtung von vertraulichen und sensiblen Unterlagen beschäftigt oder unter Vertrag genommen werden oder Zugriff auf vertrauliche und sensible Unterlagen haben, sollten in Übereinstimmung mit Folgendem sicherheitsüberprüft werden:

- a) der entsprechenden nationalen Norm; und
- b) der angemessenen Sicherheitsüberprüfungsstufe, wie vom Auftraggeber oder nationalen Richtlinien vorgegeben.

Es wird empfohlen, strenge Einstellungskontrollen einzuführen, um Sicherheitsprüfungen vor der Beschäftigung durchzuführen.

Es muss ein System vorhanden sein, das den laufenden Sicherheitsüberprüfungsprozess nach der Einstellung steuert, damit bei den Mitarbeitern neue oder verdächtige Verhaltensmuster, die ein Sicherheitsproblem darstellen könnten, ermittelt werden.

Sicherheitsüberprüfungen müssen verhältnismäßig zu den festgestellten Risiken in Bezug auf die Sensibilität der vertraulichen Unterlagen und der Schutzklasse sein.

ANMERKUNG Abhängig von der Sensibilität und/oder Schutzklasse der zu sammelnden und vernichtenden Unterlagen können vom Auftraggeber zusätzliche Sicherheitsüberprüfungen, Verifizierungen oder Zusicherungen festgelegt werden.

13.3 Schulung der Mitarbeiter

Alle an den Prozessen der Sammlung und Vernichtung von sensiblen und vertraulichen Unterlagen beteiligten Mitarbeiter müssen geschult werden.

Bediener müssen entsprechend der Schutzklasse der vertraulichen und sensiblen Unterlagen, mit denen sie Umgang haben, eine angemessene Schulung erhalten.

Der Bediener der Vernichtungsausrüstung muss in der korrekten Verwendung und Wartung der Ausrüstung geschult und regelmäßig beurteilt werden, damit das Ziel der Vernichtung erreicht wird.

Der Bediener des Fahrzeugs muss in der korrekten Verwendung eines Fahrzeugs geschult und regelmäßig beurteilt werden, damit das Ziel der Unterlagensammlung erreicht wird.

Vor Ausführung der Aufgaben muss eine fachspezifische einsatzvorbereitende Schulung durchgeführt werden. Diese muss Folgendes umfassen:

- sichere Übergabe von Datenträgern mit vertraulichen Informationen und von sensiblen Unterlagen;
- Verhindern des Verlusts von Datenträgern mit vertraulichen Informationen und von sensiblen Unterlagen;
- Erbringen einer Dienstleistung von hoher Qualität;
- Vervollständigen der Dokumentation;
- Betriebs- und Sicherheitsverfahren;
- für jede Schutzklasse erforderliche Schutzmaßnahmen;
- Schulung im Arbeits- und Gesundheitsschutz;
- Zwischenfallmanagement und Verhalten im Notfall.

Zu jedem Bediener muss eine Aufzeichnung der Schulung geführt werden, die mindestens Folgendes enthält:

- Name und Unternehmen des Bedieners;
- Datum der Beurteilung;
- Name, Position und Schulungsunternehmen der Prüfperson;
- Bestätigung, dass der Bediener zum Erreichen des Ziels der Unterlagensammlung geschult ist und/oder dass der Bediener in der Bedienung der Ausrüstung qualifiziert ist, einschließlich um das Ziel der Vernichtung zu erreichen.

Eine Auffrischungsschulung muss regelmäßig für alle Bediener durchgeführt werden, die entweder an den Sammel- und/oder Vernichtungsprozessen beteiligt sind.

Es wird empfohlen, dass die Auffrischungsschulung der Bediener mindestens einmal im Jahr durchgeführt wird.

Dokumentierte Aufzeichnungen aller Auffrischungsschulungen müssen geführt werden und Folgendes enthalten:

- Name und Unternehmen des Bedieners;
- Datum und Uhrzeit der Beurteilung;
- Name, Stellenbezeichnung/Position und Unternehmen der Prüfperson;
- Bestätigung, dass der Bediener erfolgreich die Auffrischungsschulung abgeschlossen hat.

Es wird empfohlen, dass Bediener, die Tätigkeiten am Standort des Auftraggebers ausführen, eine Kundendienstschulung erhalten.

13.4 Kontrolle der Fahrer des Unternehmens

Führerscheine müssen regelmäßig überprüft werden.

Das Unternehmen muss an die Fahrer die Anforderung stellen, dass sie Verurteilungen beim Führen eines Kraftfahrzeugs und relevante Erkrankungen angeben.

Die Schulung muss beaufsichtigt oder überwacht werden und Aufzeichnungen nach 13.3 geführt werden.

ANMERKUNG Möglicherweise gelten für die Überprüfungsabstände der Führerscheine von Mitarbeitern behördliche Anforderungen, nationale Normen und/oder Versicherungsvorgaben.

14 Sammlung und Transport von vertraulichen und sensiblen Unterlagen

14.1 Allgemeines

Die zu sammelnden vertraulichen und sensiblen Unterlagen müssen ab dem Sammelpunkt bis zum Abschluss der Vernichtung vor dem Zugriff Unbefugter geschützt werden.

Die Sammlungen müssen durch uniformierte und entsprechend geschulte Mitarbeiter, die einen Ausweis mit Bild mitführen, durchgeführt werden.

Fahrzeuge und Ausrüstung, die für die Sammlung und den Transport von vertraulichen und sensiblen Unterlagen verwendet wird, müssen gebrauchstauglich sein und in Übereinstimmung mit den Empfehlungen des Herstellers gewartet werden.

Es muss Verfahren geben, die regelmäßige Prüfungen der Fahrzeuge und der wesentlichen Ausrüstung ermöglichen. Mit Vernichtungsausrüstung ausgestattete mobile Fahrzeuge für die Vernichtung müssen in Übereinstimmung mit 7.7 bewertet werden.

14.2 Mobile Fahrzeuge zum Schreddern und zur Abholung

Die nachstehenden Schutzmaßnahmen gelten sowohl für Fahrzeuge zur Abholung außerhalb des Standorts als auch für mobile Schredderfahrzeuge vor Ort.

Für die Fahrzeuge gilt:

- sie müssen entweder einen Kofferaufbau oder einen gesicherten auswechselbaren Containeraufbau haben;
- sie müssen mit abschließbaren und/oder versiegelbaren Türen ausgestattet sein, die mit geeigneten Schlössern versehen sein sollten;
- sie müssen in der Lage sein, mit dem Unternehmen und Notfalldiensten über Funk oder Telefon zu kommunizieren. Die Mitarbeiter müssen in der Lage sein, das Kommunikationsgerät sicher und rechtlich zulässig zu bedienen, während sich das Fahrzeug bewegt;
- sie müssen mit einer akustischen Diebstahlwarnanlage oder einer Wegfahrsperre ausgestattet sein, die aktiviert sein muss, wenn das Fahrzeug unbeaufsichtigt ist;
- sie müssen mit einem Fernortungsgerät ausgestattet sein, das dem Unternehmen oder gegebenenfalls dem Unterauftragnehmer des Dienstleisters den Standort des Fahrzeug mitteilt;
- der Laderaum muss jederzeit geschlossen und verschlossen und/oder versiegelt sein, einschließlich während des Transits, außer beim Be- oder Ausladen, wenn befugte Mitarbeiter anwesend sein müssen;
- das Schreddern am Standort des Auftraggeber muss in einem gesicherten Bereich stattfinden, der bei einem mobilen Schredderfahrzeug das Schredderfach darstellt, sofern es von einer geschlossenen Tür gesichert ist;
- das Fahrerhaus darf niemals unverschlossen und unbeaufsichtigt gelassen werden;
- alle Transportfahrzeuge müssen mit geeigneten mit dem Auftraggeber vereinbarten Sicherheitsverfahren geschützt werden und einen Kofferaufbau haben;