GDD-RATGEBER

4. AUFLAGE

Datenschutzgerechte Datenträgervernichtung

- nach dem Stand der Technik -

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

Datenschutzgerechte Datenträgervernichtung

- nach dem Stand der Technik -

Datenschutzgerechte Datenträgervernichtung
- nach dem Stand der Technik -

4. Auflage, 2019
Herausgeber: Gesellschaft für Datenschutz und Datensicherheit e.V.

GDD-Arbeitskreis „Datenträgervernichtung“

Gerhard Friederici, Rhenus Office Systems GmbH
Thomas Häberlen, Bundesbeauftragter für Datenschutz und Informationsfreiheit (BfDI)
Andreas Sachs, Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
Stefan Sander, SDS Rechtsanwälte Sander Schöning PartG mbB
Rudolf Schick, Bundesamt für Sicherheit in der Informationstechnik (BSI)
Michael Stapel, Rhenus Data Office GmbH
Hermiona Zeller, Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Gerhard Stampe, MERANTIS DataSec GmbH,
Leiter des Arbeitskreises

- Alle Rechte vorbehalten -

© 2019 Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)
Heinrich-Böll-Ring 10 • 53119 Bonn

Telefon: (0228) 96 96 75 00
Telefax: (0228) 96 96 75 25
E-Mail: info@gdd.de
Internet: www.gdd.de

Nachdruck und Vervielfältigung jeder Art sind nur mit ausdrücklicher Genehmigung der GDD gestattet.

Vorwort zur 4. Auflage

Seit dem Erscheinen der 3. Auflage des GDD-Ratgebers zur datenschutzgerechten Datenträgervernichtung in 2014 hat sich einiges getan.

Eine neue internationale Norm zur Datenträgervernichtung (ISO/IEC 21964), die EU-DS-GVO, das neue BDSG sowie Änderungen des § 203 StGB finden in dieser Auflage Berücksichtigung.

Die Vorgängernorm, DIN 32757-1, die seit 1985 existiert und als eine reine Maschinennorm für die Hersteller von Schriftgutvernichtern entstand, hatte sich bis 2012 zu einer Weltnorm entwickelt.

Im August 2009 wurde in Deutschland die europäische Norm EN15713 veröffentlicht, die für einige Verwirrung sorgte.

Dieser europäische Standard war hinsichtlich des Stands der Technik, fehlender Schutzbedarfe und seines teilweise informativen Charakters alles andere als ein Fortschritt.

Die Norm DIN 32757-1 ist Geschichte! Die Norm EN15713 wurde am Markt nicht akzeptiert!

Die Entwicklung der DIN 66399-1 bis 3 hat gezeigt, wie diese Normung durch die Berücksichtigung des Stands der Technik, erhöhte Sicherheitsanforderungen für Vernichtungsmaschinen und -prozesse bei Dienstleistern bzw. Unternehmen positiv angenommen wurde.

Die DIN 66399 hat sich bei Herstellern, Dienstleistern und innerhalb der Unternehmen etabliert und maßgeblich zur mehr Sicherheit von lokalen bzw. dezentralen Vernichtungsprozessen geführt.

Dies wurde auch international anerkannt. Im August 2018 ist DIN 66399 internationalisiert worden. Die Inhalte der DIN 66399 sind seitdem in der internationalen Norm ISO/IEC 21964 übernommen worden.

Durch die Aktualisierung des Ratgebers sind Gesetzesänderungen aber auch das Einbringen von Auslegungshinweisen bei Unsicherheiten der Anwendung der DIN 66399 vom GDD-Arbeitskreis „Datenträgervernichtung“ aufgenommen und berücksichtigt worden.

Gerhard Stampe
(Leiter des Arbeitskreises)

Inhaltsverzeichnis

Vorwort zur 4. Auflage **3**

Inhaltsverzeichnis **5**

1. Prozessdefinition und Stand der Technik **9**

1.1 Prozessbeschreibung 9

1.2 Stand der Technik 10

2. Rechtliche Grundlagen **13**

2.1 Datenschutzrecht 13

2.1.1 Allgemeines 13

2.1.2 Auftragsverarbeitung 16

2.1.2.1 Grundlegendes 16

2.1.2.2 Auswahl des Dienstleisters 18

2.1.2.3 Mindestvertragsinhalte 20

2.1.3 Hinweise zum Leistungsübergabepunkt 22

2.1.4 Datenträgervernichtung mit Auslandsbezug 23

2.2 Geheimnisschutz 26

2.2.1 Privatgeheimnisse 27

2.2.1.1 Betrachtung des Lebenszyklus einer geheimen Information 27

2.2.1.2 Gesetzliche Erlaubnis zur Weitergabe der geheimen Information 28

2.2.1.3 Erweiterung des Kreises der Schweigepflichtigen 29

2.2.1.4 Detailfragen zur gesetzlichen Erlaubnis zur Weitergabe 30

2.2.2 Geschäfts- und Betriebsgeheimnisse 33

2.2.3 Staatsgeheimnisse (Schutz von Verschlusssachen) 34

2.3 Aus anderen Gründen notwendige Vertragsklauseln 35

3. Der Weg zum neuen Standard der Datenträgervernichtung **37**

3.1 ISO/IEC 21964 37

3.2 DIN 66399 37

3.2.1 DIN 66399 Teil 1 38

3.2.1.1 Schutzklassen 39

3.2.1.2 Sicherheitsstufen 41
3.2.1.3 Zuordnung von Schutzklassen und Sicherheitsstufen 43
3.2.1.4 Einflussgrößen für die Rekonstruktion von Informationen 44
3.2.1.5 Erhöhung der Sicherheitsstufe 45
3.2.2 DIN 66399 Teil 2 46
3.3 EN 15713 48
3.4 DIN 32757 49

4. Sicherheitskonzept 51

4.1 Sicherheitskonzept technische und organisatorische Maßnahmen 51
4.2 Zertifizierungen im Sinne des Datenschutzrechts 51
4.2.1 Grundlegendes 52
4.2.2 Werbung mit Zertifizierungen 53
4.3 Zertifizierungen in Bezug auf technische Normen 54
4.3.1 Grundlegendes 55
4.3.2 Zertifizierung in Bezug auf andere Normen 56
4.4 Testate, Prüfberichte und Ähnliches von Wirtschaftsprüfern, Datenschutzbeauftragten u.a. 57
4.4.1 Grundlegendes 57
4.4.2 Werbung mit den Ergebnissen der Prüfung von Wirtschaftsprüfern 58

5. FAQ/Handlungsempfehlungen 61

5.1 Auslegung der Schutzklasse 3 61
5.2 Berücksichtigung ökologischer Aspekte 62
5.3 Berücksichtigung der Größe eines Datenträgers 62
5.4 Einsatz von Verbrennungsanlagen 62
5.5 Erläuterung der Begriffe Entsorgung und Vernichtung 63
5.6 Vorgehensweise zu verschlüsselten Datenträgern 64
5.7 Zur normativen Anforderung an Sicherheitsbehältern 64

6. Checkliste **65**

6.1 Variante 1 (Datenträgervernichtung durch den Verantwortlichen direkt) 65

6.2 Variante 2 (Datenträgervernichtung vor Ort durch Dienstleister) 69

6.3 Variante 3 (Datenträgervernichtung extern durch Dienstleister) 76

7. Begriffserläuterungen **87**

8. Anlagen **91**

8.1 Vertragsergänzung zur Auftragsverarbeitung 91

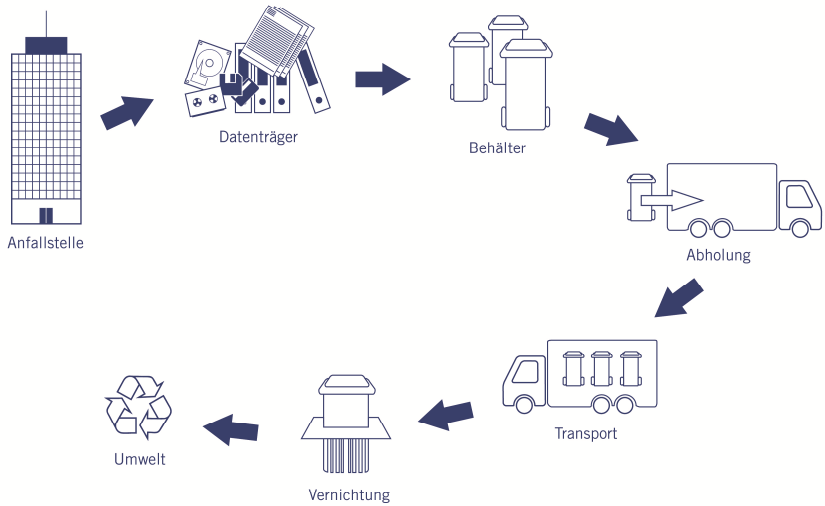
8.2 Aufbewahrungsfristen (Stand: März 2019) 101

8.3 Vereinbarung zur Geheimhaltung 108

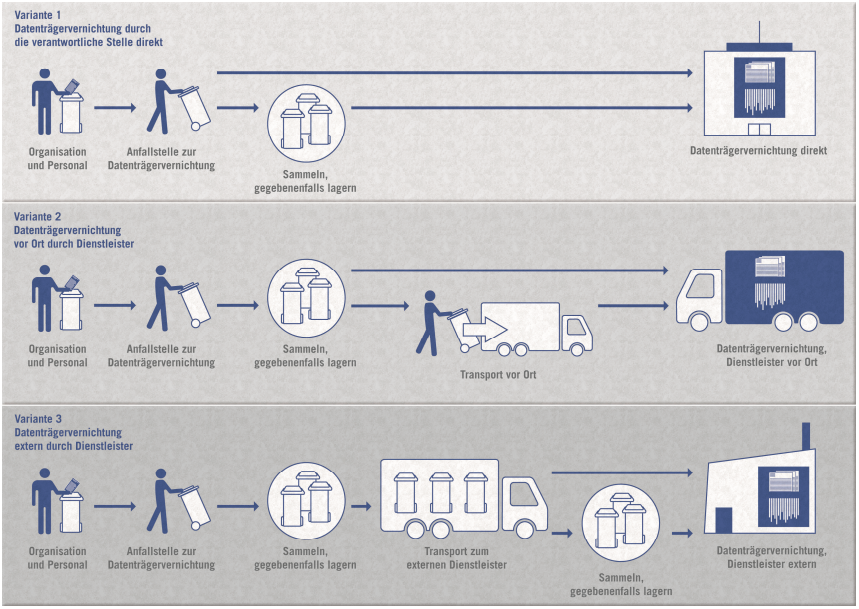
1. Prozessdefinition und Stand der Technik

1.1 Prozessbeschreibung

Datenschutzgerechte Datenträgervernichtung ist als wesentlicher Bestandteil des Vernichtungs- und Entsorgungsprozesses aufzufassen, der in seinen einzelnen Phasen zu untersuchen und zu gestalten ist. Grundsätzlich sollte nach Möglichkeit eine Beeinträchtigung der unmittelbaren Funktionsfähigkeit von Datenträgern in den frühen Phasen des Vernichtungsprozesses (Anfall und Sammlung) erfolgen. So wird die Attraktivität der Datenträger in Bezug auf Entwendung geschmälert und für die nachfolgenden Prozessschritte eine Basissicherheit erreicht.



In der Praxis kommen verschiedene Prozessvarianten der Datenträgervernichtung zum Einsatz. So kann der Verantwortliche die Vernichtung in Eigenregie durchführen oder durch einen Dienstleister entweder beim Verantwortlichen oder extern auf dem Betriebsgelände des Dienstleisters durchführen lassen (Variante 1-3). Die einzelnen Varianten werden hierbei in unterschiedliche Teilprozesse gegliedert. Die dem entsprechenden Teilprozess zugeordneten Maßnahmen (vgl. Checkliste unter Abschnitt 6.) müssen im Rahmen der Umsetzung erfüllt werden.



1.2 Stand der Technik

In der Regel läuft der Prozess vom Anfall des zu vernichtenden Materials bis zur umweltverträglichen Entsorgung arbeitsteilig ab. Werden Dienstleister in den Prozess einbezogen, ist die Verantwortungsabgrenzung zwischen Auftraggeber und Auftragnehmer klar zu regeln. Aufgrund von Rechtsvorschriften sind in diesem Prozess vor allem technisch-organisatorische Maßnahmen zu ergreifen, die die Qualität der

Abläufe im Allgemeinen und die des Dienstleistungsunternehmens im Besonderen charakterisieren.

In Anlehnung an Art. 32 DS-GVO wird von folgender Definition ausgegangen:

Die technischen und organisatorischen Maßnahmen müssen zur datenschutzgerechten Vernichtung von Datenträgern (Papier, magnetischen Datenträgern, Halbleiterspeichern etc.) unter Berücksichtigung des **Stands der Technik** und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das der Art der zu schützenden Daten angemessen ist. Dabei sind neben dem Risiko einer unzureichenden Löschung auch die vom Gesamtprozess ausgehenden Risiken zu betrachten.

Aus dieser Begriffsbestimmung sind zunächst zwei Fragen abzuleiten, die in den relevanten Gesetzen und Standards gar nicht oder nur unzureichend geklärt sind:

1. Was ist unter „Stand der Technik“ zu verstehen?
2. Welche Schutzklassendefinition ist aus Sicht des Datenschutzes angemessen?

Zur ersten Frage schlägt der Arbeitskreis folgende Antwort vor, die sich an Begriffsbestimmungen aus der Umweltgesetzgebung anlehnt:

Stand der Technik ist der zu einem bestimmten Zeitpunkt erreichte Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung im Hinblick auf den angestrebten Schutzzweck insgesamt gesichert erscheinen lässt.

Neben dem Stand der Technik verweist Art. 32 DS-GVO darauf, dass technische und organisatorische Maßnahmen zudem unter Berücksichtigung der Höhe der Implementierungskosten zu treffen sind. Dies trägt dem Angemessenheitsprinzip Rechnung, wonach kein unbegrenzter Aufwand erforderlich ist. Die Implementierungskosten bleiben jedoch bei der Bestimmung des Stands der Technik unberücksichtigt.

In Bezug auf einen am Prozess beteiligten Dienstleister hat der Arbeitskreis folgende Aussagen getroffen:

Sicherheit durch Qualität

Um das eigene Unternehmen vor Gefahr und Schaden durch Datenmissbrauch zu schützen, bedarf es eines Sicherheits- und Kontrollsystems, das eine zuverlässige Qualität des Vernichtungs- und Entsorgungsprozesses beim Dienstleister garantiert.

Qualität durch Stand der Technik

Das Niveau der dem aktuellen Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen entspricht der Qualität des Dienstleisters und somit der Sicherheit des Verantwortlichen.

Zur zweiten Frage stellt der Arbeitskreis fest: Der hohe Schutzbedarf (Schutzklassen) personenbezogener Daten muss je nach Sensibilität

- gewährleistet,
- hohen Anforderungen genügen oder
- unbedingt gewährleistet sein

(siehe Abschnitt 3.2.1.1 Schutzklassen und Abschnitt 2 Rechtliche Grundlagen).

2. Rechtliche Grundlagen

2.1 Datenschutzrecht

2.1.1 Allgemeines

Die „Vernichtung“ von personenbezogenen Daten ist eines der ausdrücklich genannten Beispiele einer Verarbeitung i.S.v. Art. 4 Nr. 2 DS-GVO. Der Gesetzgeber unterscheidet sie a.a.O. begrifflich vom „Löschen“ von personenbezogenen Daten, auf das betroffene Personen unter den Voraussetzungen von Art. 17 DS-GVO einen Anspruch haben können. Aus derselben Norm ergibt sich zudem eine objektive Rechtspflicht des Verantwortlichen, personenbezogene Daten zu löschen. Eine Verpflichtung des Verantwortlichen zur Vernichtung gibt es in der DS-GVO hingegen nicht. Jedoch hat es sich in der Praxis bewährt, zum Zwecke des Löschens von personenbezogenen Daten die Datenträger, die diese Daten enthalten (insbesondere Papier), der Vernichtung zuzuführen.

Keine Fortsetzung in der DS-GVO fand die alte deutsche Rechtslage, nach der das Löschen hinsichtlich der Zulässigkeit privilegiert behandelt wurde (vgl. § 35 Abs. 2 Satz 1 BDSG a.F.). Sowohl das Löschen, als auch das Vernichten von personenbezogenen Daten, sind Verarbeitungen, die in jedem Einzelfall eines Erlaubnistatbestands bedürfen, zur Rechtfertigung vor dem grundsätzlichen Verbot mit Erlaubnisvorbehalt. Hier soll es jedoch offen und damit der Klärung in Wissenschaft und Rechtsprechung überlassen bleiben, ob sich ein Erlaubnistatbestand eigener Art aus Art. 17 DS-GVO ergibt oder aus dieser Norm nur die rechtliche Verpflichtung abzuleiten und der Erlaubnistatbestand zugunsten des Verantwortlichen in Art. 6 Abs. 1 Satz 1 lit. c), Art. 9 Abs. 2 lit. f) DS-GVO zu sehen ist.

Für den Verantwortlichen in technischer Hinsicht maßgeblich sind die Anforderungen, die die Art. 24, 25 DS-GVO an die Verarbeitung der „Vernichtung“ stellen – insbesondere hinsichtlich der Auswahl der „Mittel der Verarbeitung“, die er für die Vernichtung der personenbezogenen Daten einsetzen will. Zusätzlich zu diesen Compliance-

orientierten Vorgaben („Verarbeitung gemäß dieser Verordnung“, insbesondere hinsichtlich der Grundsätze aus Art. 5 DS-GVO) sind ferner die Anforderungen von Art. 32 DS-GVO zu beachten, die auf die Bewältigung der mit der Verarbeitung einhergehenden Risiken abzielen. Zusammenfassend stellt sich insoweit die Frage, in welche Schutzklasse die zu vernichtenden Daten fallen. Dies hat sowohl Auswirkungen auf die Wahl der Sicherheitsstufen (d.h. die Partikelgröße des Materials bei der Vernichtung) als auch auf die organisatorischen Vorgaben für den Vernichtungsprozess, der sowohl vollständig beim Verantwortlichen als auch in Teilen oder im Ganzen bei Externen im Auftrag erfolgen kann.

Besonders bedeutsam sind in diesem Zusammenhang zum einen personenbezogene Daten besonderer Art, die in Art. 9 Abs. 1 DS-GVO abschließend benannt sind. Daten über strafbare Handlungen oder Entscheidungen über Strafsachen wurden nach der Wertentscheidung des EU-Gesetzgebers diesem Bereich ausdrücklich nicht zugeordnet, sondern diese sind gem. Art. 10 DS-GVO grundsätzlich nach denselben Maßstäben zu behandeln, wie „alle anderen“ personenbezogenen Daten auch. Zum anderen sind solche personenbezogene Daten besonders bedeutsam (ungeachtet ihres Inhalts, also z.B. Informationen über Straftaten, Telekommunikationsverbindungen, Bankkonten, im öffentlichen Telefonbuch nachlesbare Adressangaben), die einem speziellen Berufs- oder Amtsgeheimnis oder einer anderen besonderen Geheimhaltungspflicht des Verantwortlichen unterliegen. Im Übrigen können sich auch für Verantwortliche, die keinen Geheimhaltungspflichten unterliegen, in Bezug auf Daten, die nicht unter Art. 9 Abs. 1 DS-GVO fallen, verminderte oder gesteigerte Anforderungen aus Art. 32 DS-GVO ergeben, jeweils in Anhängigkeit von den Inhalten der zu vernichtenden personenbezogenen Daten.

Die in Kapitel 3 der DIN 66399-1 dargestellten Schutzklassen (siehe Abschnitt 3.2.1.1) enthalten Hinweise, wie anhand von Daten deren Schutzbedarf ermittelt werden kann und welchen Schutzklassen sie zuzuordnen sind. Die Definition dieser Schutzklassen lassen sich aber nicht 1:1 auf die datenschutzrechtlichen Besonderheiten abbilden. Im Allgemeinen dürfte die Wahl der Schutzklasse 2 sowie der Sicherheitsstufe 3 angezeigt sein. Abstrakte Hinweise, die unter dem Vorbehalt der Konkretisierung durch den Einzelfall stehen, ergeben sich auch aus

dem von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) verabschiedeten Standard-Datenschutzmodell (SDM) bzw. den Bausteinen des dazugehörenden Maßnahmenkatalogs. SDM-Baustein 60 befasst sich mit „Löschen und Vernichten“, liegt jedoch bislang nur im Entwurf vor und dieser auch nur seitens der Aufsichtsbehörden aus Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein und der Evangelischen Kirche Deutschlands vor und wird bislang noch nicht durch die DSK insgesamt getragen.

Zu jedem Eintrag in seinem Verzeichnis von Verarbeitungstätigkeiten i.S.v. Art. 30 Abs. 1 DS-GVO, d.h. zu jedem „Verfahren“ (als einer Vorgangsreihe von Verarbeitungen, deren Zusammengehörigkeit durch denselben „Zweck der Verarbeitung“ entsteht) hat der Verantwortliche auch einen Endpunkt zu bestimmen, mithin die Löschung oder Vernichtung der personenbezogenen Daten einzuplanen. Auch für diese letzte Verarbeitungstätigkeit eines jeden Verfahrens, deren Zeitpunkt den betroffenen Personen gem. Art. 13, 14 DS-GVO schon anlässlich der Erhebung mitzuteilen ist (Speicherdauer) und der gem. Art. 30 Abs. 1 Satz 2 lit. f) DS-GVO auch intern zu dokumentieren ist, sind die von ihm realisierten technischen und organisatorischen Maßnahmen im Hinblick auf diese Verarbeitung gem. Art. 30 Abs. 1 Satz 2 lit. g) DS-GVO zu dokumentieren (notwendigerweise jedoch nur solche zur Risikobewältigung gem. Art. 32 DS-GVO). Insoweit sei darauf hingewiesen, dass von den zur alten deutschen Rechtslage verbreiteten Ratschlägen Abstand genommen werden sollte, die zu diesem Zweck nur eine Grobskizze der Maßnahmen vorsahen. Im eigenen Interesse sollte der Verantwortliche die Maßnahmen i.S.v. Art. 32 DS-GVO ausführlich dokumentieren, weil die inhaltliche Erfüllung der Pflichten aus Art. 32 DS-GVO gem. ErwG 82 allein anhand der Papierlage kontrolliert werden können soll. Soweit es um die Auswahl von technischen und organisatorischen Maßnahmen geht, die gem. Art. 32 DS-GVO auf die Bewältigung der mit der Verarbeitung einhergehenden Risiken ausgerichtet sind, ist es zudem u.U. erforderlich, die Planung der Maßnahmen vor Aufnahme der Verarbeitung sehr strukturiert durchzuführen. Eine entsprechende Rechtspflicht des Verantwortlichen kennt Art. 35 DS-GVO als Datenschutz-Folgenabschätzung.

Zu guter Letzt sei darauf hingewiesen, dass die versehentliche Zuführung von personenbezogenen Daten zur Vernichtung – selbst bei Vorliegen eines Erlaubnistatbestands für die Vernichtung und damit deren Rechtmäßigkeit – eine Verletzung des Schutzes personenbezogener Daten i.S.v. Art. 4 Nr. 12 DS-GVO ist und u.U. zu Meldepflichten gem. Art. 33 DS-GVO bzw. Benachrichtigungspflichten gem. Art. 34 DS-GVO führen kann. Im Unterschied zur alten deutschen Rechtslage ist es nicht mehr erheblich, welche Arten von Daten von einer Verletzung des Schutzes personenbezogener Daten betroffen sind.

2.1.2 Auftragsverarbeitung

2.1.2.1 Grundlegendes

Da eine Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO auch im Vernichten personenbezogener Daten zu sehen ist, müsste ein mit dieser Vernichtung (wirtschaftlich) beauftragter Dienstleister einen eigenen Erlaubnistatbestand zu seinen Gunsten vorweisen können, falls er diese Vernichtung in der Rolle als Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO ausführen wollte. Ein solcher Erlaubnistatbestand ist jedoch regelmäßig nicht gegeben. Um zu vermeiden, eine rechtswidrige Verarbeitung i.S.v. Art. 83 Abs. 5 lit. a) i.V.m. Art. 5 Abs. 1 lit. a) DS-GVO auszuführen, muss sich der (wirtschaftlich) beauftragte Dienstleister daher zwingend in die Rolle des „Auftragsverarbeiters“ begeben.

Regelungen zur Auftragsverarbeitung sind in Art. 4 Nr. 8, Art. 28 DS-GVO enthalten. Der wirtschaftliche Auftrag allein lässt einen Dienstleister jedoch nicht in die privilegierte Rolle eines Auftragsverarbeiters gelangen. Vielmehr sind dafür zwei Voraussetzungen zu erfüllen. Einerseits muss der Vertrag mit dem Dienstleister, also der (wirtschaftliche) Auftrag, so formuliert sein, dass er die Mindestvertragsinhalte abdeckt, die von Art. 28 Abs. 3 DS-GVO gefordert werden. Andererseits muss sich der Dienstleister auch tatsächlich an die Vorgaben des Vertrags halten. Werden die Grenzen des Vertrags zur Auftragsverarbeitung (unberechtigt) überschritten, so handelt der beauftragte Dienstleister doch wieder als Verantwortlicher (vgl. Art. 28 Abs. 10 DS-GVO – im

Einzelfall zu klären ist dann noch, ob die Vernichtung mit dem (wirtschaftlichen) Auftraggeber in gemeinsamer Verantwortlichkeit ausgeführt wurde oder ein Exzess des Auftragsverarbeiters vorliegt). Berechtigterweise können diese Grenzen nur überschritten werden, sofern der Auftragsverarbeiter eigenen gesetzlichen Anforderungen unterliegt, die Verarbeitungen außerhalb der Grenzen des Auftrags erfordern (vgl. Art. 28 Abs. 3 Satz 2 lit. a) DS-GVO) – insoweit handelt er sodann als alleiniger bzw. isoliert zu betrachtender Verantwortlicher.

In vielen Fällen, so jedenfalls bei zu vernichtenden personenbezogenen Daten besonderer Art, wird es auch dem Auftraggeber an einem Erlaubnistatbestand fehlen, die Daten zur Erbringung der Leistungen dem Dienstleister gegenüber offenzulegen. Auch insoweit gilt, dass zur Vermeidung einer rechtswidrigen Verarbeitung (in Form dieser Offenlegung) i.S.v. Art. 83 Abs. 5 lit. a) i.V.m. Art. 5 Abs. 1 lit. a) DS-GVO der (wirtschaftlich) beauftragte Dienstleister in die Rolle des „Auftragsverarbeiters“ versetzt werden muss. Dann bedarf es keiner Prüfung von Erlaubnistatbeständen, weil der Austausch von Daten zwischen Auftraggeber und Auftragnehmer einer wirksamen Auftragsverarbeitung (tatbestandlich liegen je wechselseitige Offenlegungen und Erhebungen vor) ausnahmsweise nicht gegen das grundsätzliche Verbot mit Erlaubnisvorbehalt gerechtfertigt werden muss.

Aus diesen Gründen haben beide Parteien ein vitales Interesse daran, den (wirtschaftlichen) Auftrag um die Absprachen zu ergänzen, die inhaltlich bzw. thematisch von Art. 28 Abs. 3 DS-GVO gefordert werden und daran, dass der Dienstleister die „Bindung“ i.S.v. Art. 28 Abs. 3 Satz 1 DS-GVO auch tatsächlich einhält.

Die Auftragsverarbeitung ist vom Sachverhalt her regelmäßig dadurch gekennzeichnet, dass der Auftraggeber in der Regel nicht über spezielle Ressourcen verfügt und darum eine Datenverarbeitungsdienstleistung – im hier betrachteten Fall die Datenträgervernichtung einschließlich des Datenträgertransports – einem spezialisierten Auftragnehmer überträgt. Von Rechts wegen ist sie dadurch gekennzeichnet, dass die tatsächliche Ausführung einer Verarbeitung und die Verantwortung für diese i.S.v. Art. 4 Nr. 7 DS-GVO zwischen zwei Rechtsträgern auseinander fällt: Betroffene Personen können die ihnen zugedachten Rechte aus dem Kapitel III der DS-GVO (Art. 12 bis 23 DS-GVO) nur dem Auf-

traggeber gegenüber geltend machen, weil sie nur diesem als dem Verantwortlichen gegenüber bestehen. Daraus erwächst dem Auftraggeber schon aus Eigeninteresse, aber auch aufgrund gesetzlicher Pflichten, eine nicht zu unterschätzende Aufgabe, die mit gebotener Sorgfalt zu erfüllen ist. Diese beginnt mit der Auswahl des Dienstleisters.

2.1.2.2 Auswahl des Dienstleisters

In Art. 28 Abs. 1 DS-GVO heißt es, dass Verantwortliche „[…] nur mit Auftragsverarbeitern zusammenarbeiten [dürfen], die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“ Die DS-GVO behält damit die Rechtslage bei, die im deutschen Recht damals durch die Pflicht zur sorgfältigen Auswahl des Auftragnehmers in § 11 Abs. 2 Satz 1 BDSG a.F. geprägt war. Hinreichende Garantien in diesem Sinne sind keine zivilvertragsrechtlichen „Garantien“, sondern – unter Berücksichtigung von ErwG 81 DS-GVO – Eigenschaften des Auftragnehmers, wie z.B. Fachwissen, Zuverlässigkeit und Ressourcen. Die Auswahlentscheidung bzw. die Details ihres Zustandekommens ist vom Verantwortlichen intern zu dokumentieren (Art. 5 Abs. 2 DS-GVO). Insoweit sollten Verantwortliche sich vor einer Auftragsvergabe (bzw. bei regelmäßig wiederkehrenden Vergaben, regelmäßig wiederholt) danach erkundigen, ob diese an sie gerichtete Verpflichtung aus Art. 28 Abs. 1 DS-GVO ggf. zwischenzeitlich durch die Veröffentlichung von genehmigten Verhaltensregeln konkretisiert wurde (Art. 28 Abs. 5, Art. 40 DS-GVO). Bei bereits erteilten Aufträgen kann u.U. die Erfüllung der an den Verantwortlichen gerichteten Verpflichtung aus Art. 28 Abs. 1 DS-GVO im Einzelfall durch einen Privaten unabhängig geprüft und durch eine Zertifizierung attestiert werden (Art. 28 Abs. 5, Art. 42 DS-GVO).

Nur am Rande bemerkt sei hier, dass die alte deutsche Rechtslage in der DS-GVO keine Fortsetzung fand, nach der der Auftraggeber sich nach der Auswahl des Auftragnehmers, aber vor dem Beginn der Auf-

tragsausführung und sodann regelmäßig von den beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen (§ 11 Abs. 2 Satz 4 BDSG a.F.) und das Ergebnis dieser Überprüfungen dokumentieren musste (§ 11 Abs. 2 Satz 5 BDSG a.F.).

Um intern die begründete Entscheidung treffen zu können, dass ein bestimmter, ins Auge gefasste Dienstleister hinreichende Garantien i.S.v. Art. 28 Abs. 1 DS-GVO bietet, gibt es verschiedene Möglichkeiten zur Herleitung einer solchen Begründung. Nicht übersehen werden darf jedoch, dass längst nicht in allen Fällen der Verantwortliche die Fachkunde und Ressourcen hat, um die realisierten Maßnahmen des Auftraggebers zu beurteilen:

- Durch den Auftragnehmer wird ein überprüfbares Sicherheitskonzept vorgelegt, von dessen Einhaltung sich der Auftraggeber vor Ort überzeugt und dies dokumentiert.
- Durch den Auftragnehmer wird ein überprüfbares Sicherheitskonzept vorgelegt, das der Auftraggeber durch einen sachverständigen Dritten vor Ort überprüfen lässt (sogenanntes Kunden-Audit oder Zweiparteien-Audit). Die Verpflichtung, den sachverständigen Dritten geeignet auszuwählen, trifft dabei den Auftraggeber. Auch hier ist das Ergebnis zu dokumentieren.
- Der Auftragnehmer hat seine technisch-organisatorischen Maßnahmen in einem Drittparteien-Audit durch einen unabhängigen Auditor überprüfen lassen (z.B. einem Datenschutz-Audit) und legt ein entsprechendes Zertifikat oder Testat vor. Da die Art und der Umfang der Prüfung hier durch den Auftragnehmer festgelegt werden, trifft den Auftraggeber die Pflicht, das Zertifikat bzw. Testat im Hinblick auf die Unabhängigkeit des Auditors bzw. Zertifizierers sowie im Hinblick auf Art und Umfang der Prüfung zu bewerten. Dazu ist es erforderlich, dass dem Auftraggeber die erforderlichen Informationen aus dem Auditierungsverfahren zur Verfügung gestellt werden.

2.1.2.3 Mindestvertragsinhalte

Der (wirtschaftliche) Auftrag zur Datenträgervernichtung wird seiner Rechtsnatur nach zumeist ein Dienst- oder Werkvertrag sein, ggf. auch ein Kaufvertrag mit Nebenleistungspflichten. Dies hängt von der Formulierung des Vertrags im Einzelfall ab – ist jedoch für die Anwendung von Art. 28 DS-GVO unerheblich. Vertragsrechtlich zu beachten ist (z.B. mit Blick auf § 125 BGB), dass Art. 28 Abs. 9 DS-GVO für den Vertrag eine gesetzliche Formvorschrift enthält.

In der Anlage 8.1 ist ein Muster für eine Vertragsergänzung enthalten.

Wegen der Mindestvertragsinhalte, die in den Formulierungen abgebildet werden müssen, sei auf Art. 28 Abs. 3 DS-GVO verwiesen. Insoweit seien vier Punkte herausgegriffen und ergänzend erläutert:

Schlaglicht: „Zwecke der Verarbeitung“

Die von Art. 28 Abs. 3 Satz 1 DS-GVO geforderten auftragsspezifischen Festlegungen sind für den Auftragnehmer „individuelle“ Vereinbarungen, da sie inhaltlich vom jeweiligen Auftraggeber vorgegeben bzw. in die Verhandlungen eingebracht werden. Als Zwecke der Verarbeitung vertraglich festzuschreiben sind die Zwecke, die der Verantwortliche inhaltlich mit der Verarbeitung verfolgt. Die Inhalte, die gem. Art. 28 Abs. 3 Satz 1 DS-GVO zu vereinbaren sind, kann der Verantwortliche aus seinem Verzeichnis i.S.v. Art. 30 Abs. 1 DS-GVO entnehmen, im Kontext des „Verfahrens“ bzw. der „Verarbeitungstätigkeiten“, in dem bzw. denen er die Vernichtung durch den Auftragnehmer ausführen lässt (vgl. DSK Kurzpapier Nr. 1 zu Art. 30 DS-GVO). Die vom Auftragnehmer verfolgten wirtschaftlichen Zwecke, mithin die Erbringung der vertragsgemäßen Leistung o.ä. Formulierungen, gehören nicht erwähnt. Im Gegenteil, die Erwähnung eines Zwecks im Vertrag, den der (dann vermeintliche) Auftragsverarbeiter mit der Verarbeitung verfolgt, führt von einer Auftragsverarbeitung weg und hin zu einer gemeinsamen Entscheidung über den Zweck der Verarbeitung, mithin zu einer Verarbeitung in gemeinsamer Verantwortlichkeit.

Schlaglicht: „Weisungsrechte“

Wenngleich die alte deutsche Rechtslage eine wesentlich präziser formulierte Anforderung in § 11 Abs. 2 Satz 2 Nr. 9 BDSG a.F. enthielt, gilt nach wie vor, dass der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält, vertraglich zu vereinbaren ist. Denn in Art. 28 Abs. 3 Satz 2 lit. a) DS-GVO wird zwar die Existenz eines Weisungsrechts des Verantwortlichen vorausgesetzt. Nähere Spezifizierungen sind dort jedoch nicht niedergelegt. Vielmehr ist zu konstatieren, dass die DS-GVO an keiner Stelle den Inhalt bzw. den Bezugspunkt oder den Umfang bzw. die Reichweite des Weisungsrechts regelt. Für die Verantwortlichkeit sind Entscheidungen über die Zwecke und Mittel einer Verarbeitung sowie Entscheidungen über die Frage konstitutiv, ob eine Verarbeitung überhaupt stattfindet. Weisungsrechte diesbezüglich liegen insoweit nahe, müssen jedoch im Vertrag mit dem Gegenleistungsinteresse des Auftragnehmers in Ausgleich gebracht werden (Äquivalenzinteresse). In Art. 28 Abs. 3 Satz 2 lit. a) DS-GVO geht die DS-GVO jedoch selbst davon aus, dass es Verarbeitungen durch den Auftragsverarbeiter „außerhalb des Auftrags“, d.h. entgegen vertraglicher Vereinbarungen oder den diese ergänzenden (Einzel-)Weisungen geben kann und darf, soweit der Auftragsverarbeiter zu solchen Verarbeitungen gesetzlich verpflichtet ist. Damit wird der Umfang der Weisungsbefugnisse, der vereinbart werden sollte, jedenfalls begrenzt.

Schlaglicht: „Sicherheit der Verarbeitung“

Des Weiteren sind die vom Auftragnehmer anzuwendenden technischen und organisatorischen Sicherheitsmaßnahmen i.S.v. Art. 32 DS-GVO konkret zu vereinbaren (Art. 28 Abs. 3 Satz 2 lit. c) DS-GVO). Da der Auftragnehmer auch seinerseits selbst aus Art. 32 Abs. 1 DS-GVO verpflichtet ist (und eine nochmalige Auferlegung derselben Pflichten sinnfrei ist), folgt daraus, dass es darum geht, die Erfüllung der Pflichten des Verantwortlichen aus Art. 32 Abs. 1 DS-GVO, in Bezug auf die vertragsgegenständlichen Verarbeitungen, auf den Auftragnehmer zwecks Erfüllung zu delegieren. Dass die DS-GVO eine solche Vereinbarung fordert ist nur konsequent, begibt sich doch der Verantwortliche

gerade durch die Auslagerung der Verarbeitung der faktischen Möglichkeit, seinen Pflichten aus Art 32 Abs. 1 DS-GVO selbst nachkommen zu können. Zur Erleichterung der Formulierung kann auf ein vorhandenes Sicherheitskonzept Bezug genommen werden. Bei der Beschreibung von Sicherheitsmaßnahmen kann auf Inhalte von Normen (etwa DIN 66399 Teil III) Bezug genommen werden. Dabei sind jedoch pauschale Verweise (etwa: „Vernichtung nach DIN 66399-1/2/3“) nicht zulässig, da es auch innerhalb der Normen verschiedene Möglichkeiten zur Umsetzung von Sicherheitsmaßnahmen gibt, die bei pauschalierten Verweisen nicht festgelegt wären. Im Ergebnis würde es an konkreten Vereinbarungen zu den Leistungspflichten des Auftragsnehmers fehlen.

Schlaglicht: „Unterauftragnehmer“

Das Thema Subunternehmer ist, im Unterschied zu früher, unter Art. 28 DS-GVO nicht mehr Mindestvertragsinhalt. Denn im Unterschied zur alten deutschen Rechtslage, die kein Leitbild zur Zulässigkeit von Subunternehmern kannte, kennt die DS-GVO das Verbot des Einsatzes von Subunternehmern als gesetzliches Leitbild. Eine davon abweichende vertragliche Festlegung ist jedoch unter Beachtung der weiteren Vorgaben von Art. 28 Abs. 2 DS-GVO zulässig. Insoweit sei darauf aufmerksam gemacht, dass die Genehmigung des Einsatzes von Subunternehmen, im Generellen oder bezogen auf einen bestimmten Subunternehmer, eine strengere Formvorschrift zu erfüllen hat, als der Vertrag als solcher gem. Art. 28 Abs. 9 DS-GVO. Genehmigungen in diesem Sinne können abseits des Vertrags erteilt werden. Sollen sie jedoch direkt in einer Vertragsklausel enthalten sein, muss jedenfalls diese Klausel bzw. aus pragmatischen Gründen (oder auch aufgrund von §§ 125, 139 BGB) der ganze Vertrag der Formvorschrift des Art. 28 Abs. 2 DS-GVO genügen.

2.1.3 Hinweise zum Leistungsübergabepunkt

Es wurde schon darauf hingewiesen, dass der Gesamtprozess von der Entstehung des Abfallmaterials bis zu seiner endgültigen Vernichtung durchgängig zu organisieren ist. Besonders exakt ist die Schnittstelle

zwischen Auftraggeber und Auftragnehmer zu beschreiben. Diese ist i.d.R. mit der Transportproblematik verknüpft. In der Praxis lassen sich dazu folgende Grundmuster erkennen:

- Der Auftraggeber führt den Transport eigenverantwortlich, evtl. unter Einbindung eines selbst bestellten Subauftragnehmers durch. Der Übergabepunkt ist dann z.B. das Werkstor des Auftragnehmers bzw. dessen Entladestelle.
- Der Auftragnehmer führt den Transport unter seiner Verantwortung, evtl. unter Einbindung eines Subauftragnehmers durch. Der Übergabepunkt ist dann das beladene Fahrzeug. Manchmal stellen die Dienstleister spezielle verschließbare Behälter zur Verfügung und tauschen diese bei der Abholung aus. Dabei kann der Beladungsvorgang schon als Bestandteil bzw. Übergabepunkt des Auftrages betrachtet werden.

Schließlich gibt es, insbesondere für Einrichtungen und Unternehmen, die selbst den Besitz bzw. Gewahrsam an Akten und Datenträgern ausüben müssen oder sehr hohe Sicherheitsanforderungen stellen (z.B. Ausschluss des Transportrisikos), den Fall, dass der Dienstleister mobile Vernichtungseinrichtungen, die auf einem Fahrzeug montiert sind, einsetzt. Das Fahrzeug wird oft vor dem Unternehmensgebäude (z.B. bei Bürohochhäusern) oder im Hof des Unternehmens postiert. Der Übergabepunkt ist dort, wo die Mitarbeiter des beauftragten Unternehmens das zu vernichtende Material übernehmen.

2.1.4 Datenträgervernichtung mit Auslandsbezug

Bei der Datenträgervernichtung mit Auslandsbezug sind zwei Fälle zu unterscheiden, wobei „Ausland“ aufgrund des europäischen Binnenmarktes als Nicht-EU-Mitglied, d.h. Drittland zu verstehen ist:

1. Ein in Deutschland niedergelassener Auftraggeber lässt durch einen im Drittland ansässigen Dienstleister Datenträger vernichten.
2. Ein in Deutschland niedergelassener Dienstleister vernichtet Datenträger für einen im Drittland ansässigen Auftraggeber.

Vertragliche Absprachen, die den Ort der Verarbeitungstätigkeit eingrenzen, sind durch die DS-GVO nicht veranlasst. Gem. Art. 3 Abs. 1 DS-GVO ist die Geltung der DS-GVO nur davon abhängig, ob die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters innerhalb der EU stattfindet. Infolgedessen gelten im Fall 1 für den Auftraggeber und im Fall 2 für den Dienstleister die DS-GVO.

Am Rande bemerkt sei, dass vertragliche Absprachen, die den Ort der Verarbeitungstätigkeit eingrenzen, weiterhin zweckmäßig sein können, nicht des Datenschutzes wegen, sondern aus Gründen des Geheimnisschutzes. Soweit in den zu vernichtenden Akten- und Datenträgern „nicht-personenbezogene“ Daten verkörpert sind, ist der Anwendungsbereich der Verordnung (EU) 2018/1807 eröffnet. Das in Art. 4 dieser Verordnung enthaltene Verbot von Datenlokalisierungsauflagen gilt jedoch nicht für vertragliche Absprachen, die derartiges bewirken.

Zu Fall 1 ist darauf hinzuweisen, dass im Unterschied zu der alten deutschen Rechtslage die Regelungen zur Auftragsverarbeitung nicht auf den Bereich der EU beschränkt sind. Weder aus Art. 28 DS-GVO, noch der Begriffsbestimmung des Art. 4 Nr. 8 DS-GVO ergibt sich eine Beschränkung dahingehend, dass der Auftragsverarbeiter innerhalb der EU niedergelassen sein müsste.

Zu Fall 2 ist anzumerken, dass Art. 28 Abs. 1 DS-GVO eine Auftragsverarbeitung nur kennt bzw. zulässt, wenn sie im Auftrag eines Verantwortlichen durchgeführt wird. Dass der Auftraggeber im Drittland sitzt und für ihn die DS-GVO daher nicht gilt, hindert es nicht, den Auftraggeber im Hinblick auf die vom Dienstleister ausgeführten Verarbeitungen als Verantwortlichen zu betrachten, da Art. 4 Nr. 7 DS-GVO nicht voraussetzt, dass derjenige, der die maßgeblichen Entscheidungen trifft, innerhalb der EU niedergelassen sein müsste.

Mit Blick auf die Art. 44 ff. DS-GVO, die eine zweite Stufe der Zulässigkeitsprüfung für eine kleine Gruppe von Verarbeitungen darstellen, namentlich nur für „Offenlegungen gegenüber in Drittländern niedergelassenen Empfängern“, ist zunächst der Sachverhalt zu betrachten. Ausgehend vom typischen Geschehensablauf wird hier unterstellt, dass im Kontext der Vernichtung von Akten- und Datenträgern die in diesen

verkörperten Daten nur in eine Richtung weitergegeben werden, nämlich (je einmalig) vom Auftraggeber an den Dienstleister. Da die Art. 44 ff. DS-GVO, wie soeben dargestellt, nur für den Export von personenbezogenen Daten aus der EU gelten, sind diese Regeln unter der Annahme zum Sachverhalt nur für den Fall 1 relevant, weil es im Fall 2 lediglich zu einem Import von Daten kommt. Das Verbot mit Erlaubnisvorbehalt, mithin die Prüfung der Zulässigkeit (hier der Offenlegung gegenüber dem Dienstleister) wird hinsichtlich des für innereuropäische Sachverhalte üblichen Prüfungsmaßstabs (1. Stufe der Zulässigkeitsprüfung) dadurch bedient, dass zwischen Auftraggeber und Dienstleister im Fall 1 ein wirksamer Vertrag zur Auftragsverarbeitung geschlossen wird. Ergänzend muss der Auftraggeber in Fall 1 aber auch den Art. 44 ff. DS-GVO Rechnung tragen (2. Stufe der Zulässigkeitsprüfung). Ist der von ihm beauftragte Dienstleister in einem Drittland niedergelassen, für welches die EU-Kommission die Angemessenheit des dortigen Datenschutzniveaus festgestellt hat, ist die Offenlegung auf der zweiten Stufe gem. Art. 45 Abs. 1 DS-GVO als zulässig zu bewerten; Eine Länderliste wird von der EU-Kommission im Internet veröffentlicht unter:
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_de).

Im Übrigen sind geeignete Garantien i.S.v. Art. 46 Abs. 1 DS-GVO vorzusehen und den betroffenen Personen müssen durchsetzbare Rechte und wirksame Rechtsbehelfe verschafft werden. Derartige Garantien können sich z.B. daraus ergeben, dass Auftraggeber und Dienstleister ihren Vertrag um weitere Absprachen, namentlich Standarddatenschutzklauseln ergänzen (früher „eu model clauses“ bzw. „EU-Standardvertragsklauseln“ genannt; Achtung, insoweit besteht heute Verwechselungsgefahr, da der Begriff in Art. 28 Abs. 8 DS-GVO nunmehr anders belegt ist).

2.2 Geheimnisschutz

Losgelöst vom Datenschutzrecht zu betrachten sind andere Rechtsmaterien, die mit ihren Regelungen andere Schutzziele verfolgen. Weil diese nicht bzw. jeweils nicht ausschließlich der Verwirklichung des deutschen Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. der Verwirklichung des europäischen Grundrechts auf Datenschutz aus Art. 8 GRCh dienen, werden sie von der DS-GVO nicht im Wege des Anwendungsvorrangs verdrängt. Die im BDSG für das Verhältnis von Datenschutz und Geheimnisschutz enthaltene Kollisionsregel (die in der DS-GVO kein Pendant findet, dort aber im Wege der Auslegung inhaltlich ebenso zu erreichen ist) ist erhalten geblieben und findet sich nunmehr in § 1 Abs. 2 Satz 3 BDSG. Daraus ergibt sich, dass ein tatsächlicher Vorgang nur dann rechtmäßig ist, wenn er den Voraussetzungen aller einschlägigen Rechtsmaterien gleichzeitig genügt. Dabei sind diese einzeln zu prüfen, wobei Erlaubnistatbestände der einen Rechtsmaterie keine Auswirkung auf die andere haben. Daher ist zu prüfen, ob die Weitergabe von Akten- und Datenträgern mit geheimhaltungspflichtigen Informationen an den mit der Vernichtung zu beauftragenden Dienstleister mit Blick auf die Geheimhaltungspflichten zulässig ist.

Grundlegend angemerkt sei, dass der Anwendungsbereich der Regelungen zum Geheimnisschutz unabhängig davon ist, ob das Geheimnis aus personenbezogenen Daten besteht bzw. solche umfasst oder nicht. Nachstehend werden einige Bereiche des Geheimnisschutzes beispielhaft dargestellt, indes verstehen sich diese Erörterungen bewusst nicht als abschließende Darstellung einschlägiger Rechtsmaterien. Zudem ist anzumerken, dass die Kollisionsregel des § 1 Abs. 2 Satz 3 BDSG ausweislich ihres Wortlautes auch anzuwenden ist im Hinblick auf Geheimhaltungspflichten, die dem Verantwortlichen nicht kraft Gesetzes, sondern kraft vertraglicher Vereinbarungen obliegen, welche er eingegangen ist („Berufs- oder besondere Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen“). Darunter fällt z.B. das sog. „Bankgeheimnis“ (vgl. Ziff. 2 Abs. 1 AGB-Banken). Ob auch eine im Einzelfall vertraglich zugesagte Geheimhaltung („Verschwiegenheitsvereinbarungen“ bzw. „non disclosure agreements“) darunter fällt, mag unter-

schiedlich beurteilt werden, was jedoch für folgendes Fazit unerheblich ist: Für alle „Geheimnisse, die nicht auf gesetzlichen Vorschriften beruhen“, sondern auf Verträgen, gibt es auch nur die in den Verträgen vorgesehenen Ausnahmen oder Befugnisse, zu nenne wäre die Befugnis, die der Geheimhaltung unterliegenden Informationen einem Dritten – wie z.B. dem mit der Akten- und Datenträgervernichtung beauftragten Dienstleister – weitergeben zu dürfen. Ist für die Akten- und Datenträgervernichtung keine Ausnahme von der Geheimhaltungspflicht in den Vertrag aufgenommen, könnte es etwaig zu einem Vertragsbruch kommen. Inwieweit dieser allein Folgen zeitigt oder weitere Umstände hinzutreten müssen, ist separate Frage. Da es insoweit auf die Verträge ankommt, können hier keine weiteren Hinweise gegeben werden.

2.2.1 Privatgeheimnisse

Einigen Berufsgruppen und Institutionen hat der Gesetzgeber besondere Geheimhaltungspflichten auferlegt, weil sie Informationen aus dem persönlichen Lebens- und Geheimbereich verarbeiten. Es handelt sich vorrangig um solche sozial und wirtschaftlich bedeutsamen Berufe und Institutionen, zu denen der Einzelne ein besonderes Vertrauensverhältnis aufbauen können muss. Die Pflichten dieser Berufsgruppen und Institutionen sind in der Regel im jeweiligen Berufsrecht bereichsspezifisch geregelt. Die Verpflichtung zum Schutz von Privatgeheimnissen ergibt sich jedoch für alle Berufsgruppen und Institutionen zentral aus § 203 StGB. Die dort genannten Personen werden häufig auch als Berufsgeheimnisträger bezeichnet.

2.2.1.1 Betrachtung des Lebenszyklus einer geheimen Information

Wesentliche Begründung für die Relevanz dieser Rechtsmaterie ist die Erkenntnis, dass ein sorgsamer Umgang mit den der Geheimhaltungspflicht unterliegenden Informationen, über den gesamten Lebenszyklus der Information hinweg (von ihrer Beschaffung bzw. Generierung bis hin zur Löschung bzw. Vernichtung), ein integraler Bestandteil einer

jeden derartigen beruflichen oder dienstlichen Tätigkeit ist. Daher müssen die besonderen Geheimhaltungspflichten auch bei der Datenträgervernichtung durch den Berufsgeheimnisträger berücksichtigt werden. Es muss eine höhere Schutzklasse für die Daten und demzufolge höherwertige Vernichtungsverfahren als üblich ausgewählt werden (siehe dazu auch schon beim Datenschutzrecht, Allgemeines, sowie siehe oben unter Schutzklassen). Die Qualität der Vernichtung muss der Sensibilität der Daten entsprechen. Im Allgemeinen ist eine Vernichtung nach Schutzklasse 3 erforderlich, mindestens ist die Sicherheitsstufe 4 für die Partikelgröße zu erreichen. Dabei ist nicht relevant, ob die hierzu verwendete Technik im Eigentum des Berufsgeheimnisträgers ist oder nicht.

Entscheidet sich ein Berufsgeheimnisträger, die Vernichtung nicht selbst durchzuführen, sondern einen Dienstleister mit dieser Leistung zu beauftragen (Auslagerung), wirkt dieser Dienstleister an der beruflichen oder dienstlichen Tätigkeit mit, die für die Geheimhaltungspflichten konstitutiv ist. Die Bewertung als „Mitwirkung“ ergibt sich gerade daraus, dass der Umgang mit den Informationen über den gesamten Lebenszyklus hinweg integraler Bestandteil der Tätigkeit des Berufsgeheimnisträgers ist.

2.2.1.2 Gesetzliche Erlaubnis zur Weitergabe der geheimen Information

Ob ein Berufsgeheimnisträger die Datenträgervernichtung auslagern darf, ist in § 203 StGB nicht „negativ bzw. begrenzend“ geregelt. Ob die Tätigkeit ausgelagert wird, ist der freien unternehmerischen Entscheidung des Berufsgeheimnisträgers überlassen und wird durch keine Vorgaben präjudiziert. Dass ein Berufsgeheimnisträger die der Geheimhaltungspflicht unterliegenden Informationen einem Dienstleister (auch zum Zwecke der Vernichtung derselben) zugänglich machen darf, bedarf jedoch – gerade aufgrund des Geheimnisschutzes – einer „positiven bzw. gestattenden“ Regelung. Unbeschadet der Möglichkeit, dass der im Hinblick auf das Geheimnis Verfügungsberechtigte einem Offenbaren gegenüber dem mitwirkenden Dienstleister zustimmen (und

damit den Geheimnisschutz aufheben) kann, durch eine sog. Schweigepflichtentbindungserklärung, sieht § 203 Abs. 3 Satz 2 StGB im Generellen für Berufsgeheimnisträger und für alle ihrer jeweiligen Geheimhaltungspflicht unterliegenden Informationen die Erlaubnis vor, dem an ihrer beruflichen oder dienstlichen Tätigkeit mitwirkenden Dienstleister die Informationen offenbaren zu dürfen. Die Erlaubnis erstreckt sich, soweit das Offenbaren für die Inanspruchnahme der Tätigkeit des Dienstleisters erforderlich ist.

2.2.1.3 Erweiterung des Kreises der Schweigepflichtigen

Das Gesetz durchbricht jedoch mit der Erlaubnis aus § 203 Abs. 3 Satz 2 StGB, mitwirkenden Personen Privatgeheimnisse offenbaren zu dürfen, den Geheimnisschutz nicht. Denn im Gegenzug für die Erlaubnis zugunsten des Berufsgeheimnisträgers wird die mitwirkende Person in den Kreis derjenigen einbezogen, die das Privatgeheimnis bei Androhung von Strafe zu wahren haben. Dabei folgt die Strafdrohung unmittelbar aus dem Gesetz, in Anbetracht des rein tatsächlichen Umstandes, dass eine Person – z.B. ein Dienstleistungsunternehmer – an der die Geheimhaltungspflicht begründenden Tätigkeit mitwirkt.

Die „Geheimhaltungsvereinbarung“, die § 203 Abs. 4 Satz 2 Nr. 1 StGB zwischen dem Berufsgeheimnisträger und der mitwirkenden Person erfordert, ist für die Strafbarkeit der mitwirkenden Person unerheblich. Mit dem Abschluss einer solchen Vereinbarung, deren Inhalt sich aus dem Gesetz ergibt, vermeidet lediglich der Berufsgeheimnisträger ein ihm drohendes zusätzliches Strafbarkeitsrisiko. Aus den einem jeden Vertrag immanenten wechselseitigen Rücksichtnahmepflichten folgt daher auch ein klageweise durchsetzbarer Anspruch des Berufsgeheimnisträgers auf Abschluss einer Geheimhaltungsvereinbarung mit gesetzlichem Inhalt – der Abschluss dieser Vereinbarung berührt die mitwirkende Person in ihren Rechten und Pflichten nicht (sofern nicht zusätzliche Inhalte vereinbart werden).

In der Anlage 8.3 ist ein entsprechendes Vertragsmuster enthalten.

2.2.1.4 Detailfragen zur gesetzlichen Erlaubnis zur Weitergabe

Inhalt bzw. Reichweite der Erlaubnis aus § 203 Abs. 3 Satz 2 StGB sind derzeit noch nicht höchstrichterlich geklärt. Abzuwarten bleibt, ob sich der Maßstab „soweit erforderlich“ auf den konkreten Dienstleister bzw. die konkrete Leistung bezieht oder sich im Gegensatz dazu im Generellen auf Leistungen dieser Art bezieht. Unklar ist in diesem Zusammenhang auch, ob vor dem Maßstab der „Erforderlichkeit“ technische und organisatorische Maßnahmen gleichwertig sind. Der Arbeitskreis vertritt in diesem Zusammenhang die Auffassung, dass unter einer Tätigkeit eine Leistungsart (hier: Datenträgervernichtung) zu verstehen ist und eine differenzierte Betrachtung der in Anspruch genommenen Dienstleistungen geboten ist. Bei der Prüfung der Erforderlichkeit sind vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts strenge Maßstäbe anzulegen und insbesondere technische Zugriffsbeschränkungen zu berücksichtigen (vgl. BVerfG, Beschluss vom 18.04.2007, 2 BvR 2094/05, Abs. 42; Beschluss vom 13.10.2009, 2 BvR 256/09, Abs. 15; Beschluss vom 20.05.2010, 2 BvR 1413/09, Abs. 6). Die Erforderlichkeit des Offenbarens liegt für die Leistungsart Datenträgervernichtung nicht vor, weil auf dem Markt bereits verschiedene Verfahren etabliert sind, welche den Zugriff durch Mitarbeiter des Dienstleisters und die damit verbundene Möglichkeit zur Kenntnisnahme von Privatgeheimnissen ausschließen. Demnach genügen organisatorische Maßnahmen, wie z.B. Regelungen, die den Zugriff auf Datenträger oder die Kenntnisnahme von Daten verbieten (z.B. über eine Arbeitsanweisung oder zusätzliche Verpflichtung), den besonderen Anforderungen nicht (vgl. auch Abschnitt 5 FAQ / Handlungsempfehlungen). Die abschließende Klärung wird Wissenschaft und Rechtsprechung überlassen bleiben, ob die Passage ([…] „soweit“ dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen „erforderlich“ ist […]) zwingende Vorgaben für die Beschaffenheit der Leistungen mitwirkender Personen macht.

Ungeachtet der Frage, ob ein Offenbaren von geheimhaltungspflichtigen Informationen gegenüber einem mitwirkenden Dienstleister kraft Gesetzes oder aufgrund der Willensbekundung des Verfügungsberechtigten erlaubt ist, ist darauf aufmerksam zu machen, dass Informationen nicht offenbart werden, wenn eine Kenntnisnahme nicht möglich

ist. Die Vermeidung der Möglichkeit einer Kenntnisnahme von den zu vernichtenden Informationen durch den mitwirkenden Dienstleister ist in verschiedener Weise realisierbar:

- Maschinenlesbare Datenträger wie Festplatten, optische Speichermedien, Speichersticks etc. können ohne ein Offenbaren i.S.v. § 203 StGB durch einen Dienstleister vernichtet werden, wenn ihr Inhalt nach dem Stand der Technik verschlüsselt ist und der Dienstleister keinen Zugriff auf die Schlüssel hat (siehe hierzu Kapitel 5).
- Der Berufsgeheimnisträger kann die Datenträger mit der vom Dienstleister gemieteten Technik selbst vernichten bzw. durch einen „berufsmäßig tätigen Gehilfen“ (z.B. Sprechstundenhilfe, Steuerfachanstellte/r etc.) vernichten lassen. Wird die Technik von Personal des Dienstleisters begleitet, z.B. nicht nur zwecks Anlieferung und Abtransport sondern auch für eine Einweisung an der Maschine, ist es wichtig, dass bis zum Abschluss der Vernichtung nur der Berufsgeheimnisträger bzw. seine Gehilfen auf die Datenträger zugreifen können.

Folgende Tipps gelten insbesondere für die Datenträgervernichtung durch die Träger von Berufs- und Amtsgeheimnissen i.S.v. § 203 StGB:

- Der gesamte Prozess der Datenträgervernichtung ist durchgängig sicher zu gestalten und beginnt innerhalb des Organisationsbereichs des Berufsgeheimnisträgers. „Im eigenen Hause“ muss dafür Sorge getragen werden, dass Unbefugte keinen Zugriff auf zu vernichtendes Datenträgermaterial haben können.
- Für die Vernichtung von Informationen auf Papier werden nachfolgend die Varianten dargestellt: Die Übergabe an das beauftragte Unternehmen erfolgt in einem rundum geschlossenen Gesamtprozess gemäß DIN 66399.
    - Die erste Möglichkeit besteht darin, dass das beauftragte Unternehmen mobile Technik direkt auf dem Gelände des Auftraggebers platziert. Die verschlossenen Behälter werden in das Spezialfahrzeug eingebracht,

der Verschluss wird automatisch im Inneren des Fahrzeuges geöffnet und in den Schredder verbracht, danach verwirbelt und zu Ballen gepresst. Der Mitarbeiter des beauftragten Unternehmens kann diesen Prozess steuern und kontrollieren, ohne dass er dabei gespeicherte Daten zur Kenntnis nehmen kann. Die gepressten Papierballen werden dem Auftraggeber zurückgegeben oder in den Recyclingprozess überführt.

- Die zweite Möglichkeit besteht darin, dass die verschlossenen Behälter in ein geschlossenes Fahrzeug des beauftragten Unternehmens geladen werden und die Vernichtung am Ort des Dienstleisters geschieht. Wenn der gesamte Transport- und Vernichtungsprozess durch den Berufsgeheimnisträger bzw. die bei ihm berufsmäßig tätigen Gehilfen begleitet wird und die Vernichtung beim Dienstleister ohne Zwischenlagerung und unter Beobachtung bzw. Durchführung des Begleiters unmittelbar vorgenommen wird, sind die gesetzlichen Rahmenbedingungen ebenso erfüllbar.

- Bei wiederbeschreibbaren Datenträgern, insbesondere bei Festplatten und anderen elektrischen Speichermedien, sollte der Berufsgeheimnisträger die gespeicherten Inhalte auf den zu vernichtenden Datenträgern einer angemessenen Verschlüsselung zuführen, bevor die Übergabe an den Dienstleister erfolgt; Letzteres ist jedoch nur bei intakten Datenträgern möglich.
- Fällt diese Möglichkeit wegen nicht mehr mit Betriebssystemunterstützung oder Spezialsoftware ansprechbarer Datenträger aus, dann ist genauso wie bei papiernen Datenträgern zu verfahren (Schreddern vor Ort, verschlossene Behältnisse und Lagerräume, zuverlässiges und geschultes Personal, Verfahrensanweisung).
- Auch der gem. § 203 Abs. 3 Satz 2 StGB erlaubte Vorgang sollte mit einer Verschwiegenheitsvereinbarung flankiert werden, damit der Berufsgeheimnisträger das ihm aus der Einschaltung des Dienstleisters neben seiner originären

Strafbarkeit aus § 203 Abs. 1, 2 StGB zusätzlich erwachsende Strafbarkeitsrisiko aus § 203 Abs. 4 Satz 2 Nr. 1 StGB vermeidet.

2.2.2 Geschäfts- und Betriebsgeheimnisse

Soweit es um Informationen geht, die für andere Unternehmen Geschäfts- und Betriebsgeheimnisse sein können, werden diese vom hier betrachteten Auftraggeber des Dienstleisters, der die Akten- und Datenträgervernichtung ausführen soll, regelmäßig aufgrund einer vertraglich begründeten Geheimhaltungspflicht geschützt (inwieweit diese der Beauftragung des Dienstleisters entgegensteht: s.o.).

Hingegen ist in Bezug auf Informationen, die Geschäfts- und Betriebsgeheimnisse des hier betrachteten Auftraggebers sind, festzustellen, dass die Regelungen zum Schutz von Geschäfts- und Betriebsgeheimnissen denknotwendig der Weitergabe der Informationen an den die Akten- und Datenträgervernichtung ausführenden Dienstleister nicht entgegenstehen. Denn der Auftraggeber für diese Leistungen ist selbst der Verfügungsberechtigte an diesem Geheimnis. Eine gem. § 1 Abs. 2 Satz 3 BDSG zusätzlich zum Datenschutzrecht zu beachtende Schranke ist insoweit nicht ersichtlich.

Nichtsdestotrotz muss wegen der Geschäfts- und Betriebsgeheimnisse des hier betrachteten Auftraggebers auf die neue Rechtslage unter dem Geschäftsgeheimnisgesetz (GeschGehG) hingewiesen werden. In § 2 Nr. 1 GeschGehG heißt es: „Im Sinne dieses Gesetzes ist Geschäftsgeheimnis eine Information, die (b) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist“. Diese gesetzgeberische Definition des Geheimnisses, die technische und organisatorische Maßnahmen zur Geheimhaltung als konstitutiv für den Geheimnischarakter einer Information vorsieht, setzt die Richtlinie (EU) 2016/943 in nationales Recht um, die in ihrem Art. 2 Abs. 1 lit. c) dieselbe Anforderung kennt. Insoweit wird ein Umdenken in Deutschland durch das Europarecht erzwungen: Mangels „angemessener Geheimhaltungsmaßnahmen“ ist eine Information kein Geheimnis mehr, was von wesentlicher Bedeutung mit

Blick auf ihre etwaig rechtswidrige Entwendung ist. Wichtig ist dabei die vorausschauende Planung, da zu fragen ist, ob die Informationen bereits im Tatzeitpunkt Gegenstand solcher Maßnahmen waren. Auch insoweit wird gelten müssen, dass Informationen nur dann potentiell als Geheimnisse in Betracht kommen, wenn sie über ihren gesamten Lebenszyklus hinweg (von ihrer Beschaffung bzw. Generierung bis hin zur Löschung bzw. Vernichtung) Gegenstand von angemessenen Geheimhaltungsmaßnahmen waren. Infolgedessen wird sich jede in Deutschland geschäftlich tätige natürliche oder juristische Person mit der Frage auseinandersetzen müssen, wie in ihrem Geschäftsbetrieb die sichere Löschung bzw. Vernichtung von Informationen organisiert ist.

Die Wertungen der Richtlinie (EU) 2016/943 werden auch in anderen Rechtsmaterien zu berücksichtigen sein, etwa bei Anwendung des § 67 Abs. 2 Satz 2 SGB X. Dieser kodifiziert für den dortigen Kontext die frühere deutsche Rechtsauffassung: „Betriebs- und Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben.“ Informationen, die aus sich heraus bzw. kraft Natur der Sache geheimhaltungsbedürftig sind und deshalb Geheimnischarakter haben, wird es auch dort nicht mehr geben.

2.2.3 Staatsgeheimnisse (Schutz von Verschlusssachen)

Verschlusssachen sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform, die entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung einer bestimmten Geheimhaltungsstufe zugeordnet sind.

Im Interesse der gemeinsamen Verantwortung für das Wohl des Bundes und der Länder nach § 4 Abs. 1 SÜG (Sicherheitsüberprüfungsgesetz) und eines einheitlichen Geheimschutzes in Deutschland wird auf die Verbindlichkeit der BSI TL auch in den jeweiligen Regelungen für die o.a. unterschiedlichen Zuständigkeitsbereiche gem. § 35 SÜG (Nachrichtendienste, Geschäftsbereich des BMVg, geheimschutzbetreute

Wirtschaft) sowie insbesondere der Bundesländer hingewiesen. Sofern unterschiedliche Regelungen und Umsetzungshinweise in den jeweiligen Zuständigkeitsbereichen bestehen und nicht formal vereinheitlicht werden können, sind zumindest Konsistenz, Konvergenz und Kohärenz der unterschiedlichen Regelungen angestrebt.

Die Behandlung von Verschlusssachen (VS) wird in der Verschlusssachenanweisung, herausgegeben vom Bundesministerium des Innern, Bau und Heimat, geregelt. Zur Umsetzung der Anforderung zur Vernichtung von Datenträgern mit Bezug zu Verschlusssachen steht im Bundesamt für Sicherheit in der Informationstechnik (BSI) die Geheimschutzberatung zur Verfügung.

E-Mail: geheimschutzberatung@bsi.bund.de

Im Kontext von Verträgen über Lieferungen und Leistungen können Verschlusssachen auch nicht öffentlichen Stellen zur Kenntnis gelangen. Das Geheimschutzverfahren in der Wirtschaft wird im Wesentlichen ausgestaltet durch das sog. Geheimschutzhandbuch (GHB), dessen Geltung durch Abschluss eines öffentlich-rechtlichen Vertrages zwischen Bundesministerium für Wirtschaft und Energie (BMWi) und dem Unternehmen vereinbart wird.

Unternehmen der geheimschutzbetreuten Wirtschaft wenden sich in allen Fragen zum Geheimschutz an das BMWi.

2.3 Aus anderen Gründen notwendige Vertragsklauseln

In diesem Ratgeber sei nur am Rande bemerkt, dass in den Verträgen zur Akten- und Datenträgervernichtung auch aus anderen Rechtsgründen (als dem Datenschutz und Geheimnisschutz) bestimmte Inhalte vereinbart werden müssen. Solche Gründe ergeben sich vorrangig aus dem für den Auftraggeber geltenden Recht, insbesondere soweit dieses Anforderungen an die Geschäftsorganisation bzw. im Speziellen an das Risikomanagement stellt. Dies betrifft jedenfalls die Auftraggeber, die der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht – kurz BaFin – unterliegen, welche die Aufsicht über Banken und Finanz-

dienstleister, Versicherer und den Wertpapierhandel unter einem Dach vereinigt. Denn bei der nicht nur einmaligen Inanspruchnahme der Leistungen eines Dienstleisters im Bereich der Akten- und Datenträgervernichtung liegt u.a. eine Auslagerung i.S.d. Kreditwesengesetzes (KWG) bzw. eine Ausgliederung i.S.d. Versicherungsaufsichtsgesetzes (VAG) vor. Mindestvertragsinhalte sind insoweit u.a. benannt im BaFin-Rundschreiben 09/2017 (BA) – MaRisk, dort im Allgemeinen Teil 9 und im BaFin-Rundschreiben 2/2017 (VA) – MaGo, dort im Teil 13. Da es sich bei den Dienstleistern im Bereich der Akten- und Datenträgervernichtung regelmäßig um Mehrmandantendienstleister handelt, sei abschließend darauf hingewiesen, dass laut den Sitzungsprotokollen des von der BaFin geleiteten Fachgremiums MaRisk (insb. Sondersitzung am 15.03.2018 in Bonn) der Mehrmandantendienstleister „aufsichtsrechtlich“ nicht die Verantwortung trägt. Gegenüber der Aufsicht sind die Geschäftsleiter des auslagernden Instituts für die Ordnungsmäßigkeit der Aktivitäten und Prozesse, folglich auch für damit zusammenhängende Mängel verantwortlich. Das Institut ist in der Pflicht, die Mängel unter Einbeziehung des Mehrmandantendienstleisters zu beheben bzw. darauf hinzuwirken, dass die Mängel vom Dienstleister beseitigt werden, was wiederum entsprechende Überwachungshandlungen zur Leistungserbringung und zur Einhaltung rechtlicher Vorgaben voraussetzt.

3. Der Weg zum neuen Standard der Datenträgervernichtung

3.1 ISO/IEC 21964

Das nationale Normengremium im DIN zur Akten-/Datenträgervernichtung hat die DIN 66399 der International Standardisation Organisation (ISO) vorgestellt.

Die Aussagen der DIN 66399 haben international eine hohe Akzeptanz gefunden, so dass in 2018 die drei Teile der DIN 63399 von der International Standardisation Organisation (ISO) als ISO/IEC 21964 übernommen wurden.

Im Rahmen der Überführung der DIN 66399 in die ISO/IEC 21964 wurde im Teil 1 der Norm das Kapitel zu Einflussgrößen in der Rekonstruktion neu strukturiert. Es erfolgte eine Zuordnung der Absätze zu den Punkten „Allgemeines“, „Verantwortlichkeit“ und „Anforderung“, vgl. Abschnitt 3.2.1.5.

Verantwortlich für die Festlegung der notwendigen Maßnahmen sowie die Anwendbarkeit der Regelungen für großtechnische Anlagen ist einzig der Datenbesitzer.

3.2 DIN 66399

Das Neue und Einzigartige an der neuen DIN 66399 ist der ganzheitliche Ansatz. Denn sie deckt gemeinsam mit dem Teil 3, der DIN 66399-3, erstmals explizit den gesamten Prozess der Datenträgervernichtung ab. Angefangen von der internen Sammlung/Erfassung, Zwischenlagerung über den Transport bis hin zur Vernichtung der Datenträger. Und zwar sowohl für den internen Prozess (Durchführung durch den Datenbesitzer selbst), die Vernichtung vor Ort durch einen Dienstleister als auch die vollständig externe Prozesskette (Vernichtung erfolgt zentral bei einem Dienstleister).

3.2.1 DIN 66399 Teil 1

Der Teil 1 liefert die Definitionen und Begriffe und die Faktoren, die für die Datenträgervernichtung relevant sind:

- Schutzklassen 1- 3
- Sicherheitsstufen 1-7
- Zuordnung von Schutzklassen zu Sicherheitsstufen
- Einflussgrößen für die Rekonstruktion von Informationen

Bei der Schutzbedarfsermittlung und Zuordnung von Sicherheitsstufen ist folgendes zu berücksichtigen:

> Um bei der Datenträgervernichtung dem Wirtschaftlichkeits- bzw. Angemessenheitsprinzip Rechnung zu tragen, sind die zu vernichtenden Daten in Schutzklassen einzuteilen. Diese wiederum sind ausschlaggebend für die Wahl der Sicherheitsstufe. Und weil niemand seine Daten besser kennt, als der der sie erzeugt, muss diese Zuordnung durch den Datenbesitzer selbst erfolgen.
>
> Hierbei sollten Sie beachten, dass die Wahl von Schutzklasse und Sicherheitsstufe direkten Einfluss auf die Kosten der Datenträgervernichtung hat: Es kann sogar wirtschaftlich vorteilhafter sein, die Datenträger nach Schutzklassen voneinander zu trennen. Denn dann werden ausschließlich die Datenträger in einer höheren Schutzklasse entsprechend den Vorgaben für den Prozess und die Zerkleinerung oder Vernichtung behandelt, die diesem Schutz auch wirklich bedürfen.
>
> Je höher der Grad der Vernichtung ist, desto höher ist der Energie-, Personal- und Maschinenaufwand, aber auch der Aufwand für die Wiederherstellung der Daten; bis hin zu einer Vernichtung, die eine Wiederherstellung unmöglich macht.
>
> Daher sollte diese Entscheidung nicht leichtfertig getroffen werden.

3.2.1.1 Schutzklassen

Die Anforderungen an die Datenträgervernichtung müssen den Schutzbedarf der Daten aus Daten-, Geheimschutz und Vorgaben für Geschäfts-, Betriebs- und Berufsgeheimnisse berücksichtigen. Entsprechend dem Schutzbedarf sind die Schutzklassen der DIN 66399 Teil 1 auszuwählen. Die Festlegung der Schutzklasse hat sowohl Auswirkung auf die möglichen Sicherheitsstufen als auch auf die Prozesse der Datenträgervernichtung.

Die Auswahl der Schutzklasse und der anzuwendenden Sicherheitsstufe obliegt dem Verantwortlichen, welcher für den Prozess in seiner Gesamtheit, auch bei Einbindung von Dienstleistern, verantwortlich bleibt.

Die drei Schutzklassen definieren sich nach DIN 66399 Teil 1 (auch heute noch) wie folgt, wobei hinsichtlich der dort in Bezug genommenen Legaldefinition (bis zum 24.05.2018 „Betroffener“, seit dem 25.05.2018 „betroffene Person“) in Deutschland durch die DS-GVO keine Veränderung der Bedeutung eingetreten ist:

Schutzklasse 1:

Unberechtigte Offenlegung oder Weitergabe hätte begrenzte negative Auswirkungen auf das Unternehmen.

Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass der Betroffene in seiner Stellung und in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Schutzklasse 2:

Eine unberechtigte Weitergabe hätte erhebliche Auswirkungen auf das Unternehmen und könnte gegen vertragliche Verpflichtungen oder Gesetze verstoßen.

Der Schutz personenbezogener Daten muss hohen Anforderungen genügen. Andernfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.

Schutzklasse 3:

Eine unberechtigte Weitergabe hätte ernsthafte (existenzbedrohende) Auswirkungen auf das Unternehmen und/oder würde gegen Berufsgeheimnisse, Verträge und Gesetze verstoßen.

Der Schutz personenbezogener Daten muss unbedingt gewährleistet sein. Andernfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.

Anmerkung: Die vollständigen Wortlaute finden sich in der DIN 66399:2012 Teil 1.

Beispiele:

Schutzklasse 1:

Informationen, die für größere Gruppen bestimmt sind: Arbeitspläne, Telefonlisten, allgemeine E-Mails

Schutzklasse 2:

Informationen, die nur einem kleinen Personenkreis bekannt sind: Mitarbeiter-, Kunden-, Lieferantendaten, einfache Geburtstagslisten, normale Unterlagen aus Forschungs- und Entwicklungsabteilung

Schutzklasse 3:

Informationen, die einem namentlich bekannten Kreis von Personen verfügbar sind: finanzielle Ergebnisse, Preis-, Marketingstrategien, Informationen zu Pension, Rente, Arbeitsverhältnisse, Lebenslauf, hochsensitive Unterlagen aus Forschungs- und Entwicklungsabteilung

3.2.1.2 Sicherheitsstufen

Die DIN 66399 sieht sechs Materialklassen (P, F, O, T, H, E; siehe Abs. 3.2.2) und für jedes Material sieben Sicherheitsstufen vor. Die Auswahl einer höheren Sicherheitsstufe kann durch den Schutzbedarf wesentlich beeinflusst werden. Mit höheren Sicherheitsstufen steigt der Aufwand der Vernichtung. Die Verwendung einer höheren Sicherheitsstufe wird notwendig, wenn ein höherer Schutz gegen die Wiederherstellung erforderlich ist.

Prinzipielle Eignung von Sicherheitsstufen (Datenträgerübergreifend) zu Datenkategorien:

Sicherheitsstufe (P,F,O,T,H,E)	**Geeignet für**
1	**Allgemeine Daten –** Eine Reproduktion ist ohne besondere Hilfsmittel und Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand möglich
2	**Interne Daten –** Eine Reproduktion ist nur mit Hilfsmitteln und besonderem Aufwand möglich
3	**Sensible und vertrauliche Daten –** Eine Reproduktion ist nur mit erheblichem Aufwand möglich (Hilfsmittel, Zeit, Personal)
4	**Besonders sensible und vertrauliche Daten –** Eine Reproduktion ist nur mit außergewöhnlich hohem Aufwand möglich (Hilfsmittel, Zeit, Personal)
5	**Geheim zu haltende Daten –** Eine Reproduktion ist nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen, sowie forensischen Methoden möglich
6	**Geheim zu haltende Daten, wenn außergewöhnlich hohe Sicherheitsvorkehrungen einzuhalten sind –** Eine Reproduktion ist nach dem Stand der Technik unmöglich
7	**Streng geheim zu haltende Daten, wenn höchste Sicherheitsvorkehrungen einzuhalten sind –** Eine Reproduktion ist nach dem Stand von Wissenschaft und Technik unmöglich

Visualisierung der Partikelgrößen (in mm²) der DIN 66399

Maximale Partikelgröße der Sicherheitsstufe (Regel)	Kategorie P Darstellung in Originalgröße, z.B. Papier	Maximale Partikelgröße der Sicherheitsstufe bezogen auf eine Toleranzmenge von 10%
	Sicherheitsstufe P-1 2000mm² 3800mm²	
	Sicherheitsstufe P-2 800mm² 2000mm²	
	Sicherheitsstufe P-3 320mm² 800mm²	
	Sicherheitsstufe P-4 160mm² 480mm²	
	Sicherheitsstufe P-5 30mm² 90mm²	
	Sicherheitsstufe P-6 10mm² 30mm²	
	Sicherheitsstufe P-7 5mm²	Keine Toleranz zulässig

Die vorstehende Darstellung soll die unterschiedlichen Größenverhältnisse lediglich veranschaulichen.

3.2.1.3 Zuordnung von Schutzklassen und Sicherheitsstufen

Innerhalb der Schutzklassen ist die Anwendung verschiedener Sicherheitsstufen vorgesehen.

Dargestellt sind in der Tabelle die für den Datenschutz relevanten Möglichkeiten. Die Norm DIN 66399 sieht die Anwendung der Sicherheitsstufen 1 und 2 im Bereich Datenschutz nicht vor.

In der Tabelle mit "X" gekennzeichnete Felder stellen die Vorgabe der DIN 66399 dar.

Für die Vernichtung von Dokumenten mit Bürogeräten "B" sind höhere Sicherheitsstufen empfohlen. Erläuterungen hierzu finden sind in Abschnitt 3.2.1.4.

Die Erhöhung der Sicherheitsstufe "S" ist für bestimmte Materialklassen unter Berücksichtigung der Anforderungen der Norm nach Maßgabe des Verantwortlichen möglich, vgl. 3.2.1.5. Eine Sonderstellung nimmt die Erhöhung auf die Sicherheitsstufe 4 in Schutzklasse 3 ein, da in Schutzklasse 3 die Verwendung der Sicherheitsstufe 3 originär nicht vorgesehen ist.

Sicherheitsstufe **Schutzklasse**	**3**	**4**	**5**	**6**	**7**
1	X, S				
2	X, S	X, S, B	X		
3		X, S	X, B	X	X

X = Vorgabe der Norm
B = Empfehlung bei Verwendung von Büroaktenvernichtern
S = anwendbar durch Erhöhung der Sicherheitsstufe

3.2.1.4 Einflussgrößen für die Rekonstruktion von Informationen

Diese Einflussgrößen sind:

- die Menge an Vernichtungsgut
- die Größe der Information auf dem Datenträger
- farbliche Unterschiede des Datenträgers

Sehr kleine Mengen an Vernichtungsgut (z.B. wenige Blatt Papier) oder eine kleine Schriftgröße führen zu einem verringerten Aufwand bei der Wiederherstellung der Daten, dem mit der Anwendung einer höheren Sicherheitsstufe Rechnung getragen werden muss.

So sind z.B. bei einer kleineren Schriftgröße auf einem einzelnen Papierschnipsel aus einem Schredder mehr Zeichen/Text enthalten, so dass ein Zusammensetzen des Gesamtdokuments erleichtert wird.

Ebenso ist eine höhere Sicherheitsstufe notwendig, wenn durch das zu vernichtende Material selbst, z.B. ein farblicher Unterschied einiger weniger Anteile im Vernichtungsgut, eine Vorsortierung möglich und damit die Menge des Vernichtungsguts verringert wird. Dies erhöht die Chancen der Wiederherstellung.

Praktische Versuche mit einigen Seiten eines Dokuments haben gezeigt, dass mittels Büroaktenvernichter der Stufe P-4 vernichtete Dokumente in kurzer Zeit von Hand zusammengesetzt werden können. Durch die einheitliche Größe der Partikel bei sogenannten Cross-Cut-Geräten wird die Wiederherstellung erleichtert.

Informationen aus einem Wettbewerb der U.S.-Behörde DARPA zur Wiederherstellung von Dokumenten finden sich im Internet unter:
http://archive.darpa.mil/shredderchallenge/

Daraus folgend sollte bei Schutzklasse 3 unter Berücksichtigung der dargestellten Aspekte in Erwägung gezogen werden Büroaktenvernichter der Stufe P-5 zu verwenden.

Großtechnische Anlagen, wie sie üblicherweise von Dienstleistern verwendet werden, zerkleinern Papier mittels sogenannter Desintegratoren. Das Papier wird hierbei in unregelmäßige Stücke zerschnitten bzw. zerrissen. Hierbei fallen alle Partikelgrößen von nicht unerheblichen

Mengen Staub bis hin zu Partikeln, entsprechend der gewünschten Sicherheitsstufe an. Durch die Verwendung von Siebeinsätzen in den Maschinen wird bei Desintegratoren die gewünschte Partikelgröße erzielt.

Die unterschiedlichen Partikelformen und der hohe Anteil an Partikeln, die erheblich kleiner sind als die geforderte Partikelgröße gemäß der Sicherheitsstufe, führen dazu, dass für eine Wiederherstellung notwendige Anteile an Informationen nicht mehr verfügbar sind.

Dieser Sachverhalt hat das Normengremium veranlasst, eine Erhöhung der Sicherheitsstufe im begrenzten Umfang für die Materialklassen P und F bis Sicherheitsstufe P-4, F-4 zuzulassen.

3.2.1.5 Erhöhung der Sicherheitsstufe

„Allgemeines“

Das Vermischen und Verpressen von Vernichtungsgut kann die Reproduktion erschweren. Die Information auf einem Partikel verändert sich dadurch nicht. Die Sicherheitsstufe der Maschine aus dem Prüfzeugnis nach DIN66399-2 muss hierbei bekannt sein, ggf. durch Herstellerbescheinigung.

Dem Verantwortlichen muss es jederzeit möglich sein, Proben vom Vernichtungsgut zu nehmen.

„Anforderung“

Eine Erhöhung der Sicherheitsstufe ist nur für die Materialarten P (Papier u.ä.) und F (Folien, Microfiche u.ä.) vorgesehen. Es sind mindestens 100 kg in einem Durchgang zu vernichten.

Eine Erhöhung der Sicherheitsstufe ist bis maximal Sicherheitsstufe 4 (P-4, F-4) erlaubt.

„Verantwortlichkeit“

Die Entscheidung der Nutzung dieser Regelung der Norm liegt beim Verantwortlichen. Es wird empfohlen, sich vor einer Entscheidung Partikelproben und den Vernichtungsprozess anzusehen. Die Partikel und der Prozess müssen den Anforderungen der Norm und des Verantwortlichen an den Schutzbedarf der Daten gerecht werden.

3.2.2 DIN 66399 Teil 2

Durch die neuen Anforderungen an Maschinen zur Vernichtung von Datenträgern sind die wesentlichen Fragen der Gebrauchstauglichkeit und Zuverlässigkeit geklärt. Das schafft Kontrolle, ob Datenträger vollständig vernichtet sind.

In der Norm sind die Materialien zu Klassen zusammengefasst:

Material-klasse	Darstellung / Datenträger	Beispiele
P	Informationsdarstellung in Originalgröße	Papier, Overheadfolie
F	Informationsdarstellung verkleinert	Film (Filmmaterial, Negative), Mikrofilm, Mikrofiche, Papier mit kleinen Schrifttypen
O	optische Datenträger	CD, DVD u.ä.
T	magnetische Datenträger	Disketten, ID-Karten (Magnetstreifen), Magnetbandkassetten
H	Festplatten mit magnetischem Datenträger	Festplatten, Festplattenscheiben
E	elektronische Datenträger	Chipkarten (SD-Karten etc.), Speicherbausteine, Halbleiterfestplatten (SSD), USB-Stick, mobile Kommunikationsmittel

Die Beschaffenheit, Datendichte und auch mögliche Wiederherstellungsmethoden bedingen unterschiedliche Partikelgrößen für die verschiedenen Datenträger. Generell gilt: Je höher die Informationsdichte,

desto kleiner müssen die nach der Vernichtung vorhandenen Partikel sein.

Exemplarisch die Nennung einiger Sicherheitsstufen für ausgewählte Materialien:

Papier:

Sicherheitsstufe P-3: ≤ 320 mm² oder Streifenschnitt mit 2 mm Breite
Sicherheitsstufe P-4: ≤ 160 mm² und bei Partikelschnitt maximal 6 mm breite Partikel
Sicherheitsstufe P-5: ≤ 30 mm² und bei Partikelschnitt maximal 2 mm breite Partikel
wobei ein Teil der Partikel größer sein darf:
Sicherheitsstufe P-3: 10% ≤ 800 mm²
Sicherheitsstufe P-4: 10% ≤ 480 mm²
Sicherheitsstufe P-5: 10% ≤ 90 mm²

Festplatten:

Sicherheitsstufe H-3: Datenträger verformt
Sicherheitsstufe H-4: ≤ 2000 mm²; mit 10% ≤ 3800mm²
Sicherheitsstufe H-5: ≤ 320 mm²; mit 10%≤ 800mm²

Elektronische Datenträger:

Sicherheitsstufe E-3: ≤ 160 mm²; mit 10% ≤ 480mm²
Sicherheitsstufe E-4: ≤ 30 mm²; mit 10% ≤ 90mm²
Sicherheitsstufe E-5: ≤ 10 mm²; mit 10% ≤ 30mm²

In den Sicherheitsstufen E-4 und höher ist das Teilen des eigentlichen Datenträgers, den Chip, gefordert.

Anmerkung: Die vollständigen Angaben finden sich in der DIN66399:2012 Teil 2.

3.3 EN 15713

Im August 2009 wurde in Deutschland die europäische Norm EN 15713 veröffentlicht. Allerdings stellt dieser europäische Standard alles andere als einen Fortschritt dar.

Aus folgenden Gründen halten wir die EN 15713 für ungeeignet:

1. Die Formulierungen der EN 15713 sind unverbindlich.
   Die physischen Eigenschaften werden zur Unterscheidung verwendet, anstatt auf das Schutzbedürfnis der auf einem Datenträger enthaltenen Daten abzuzielen.
2. Die Zuordnung der Materialien zu den Kategorien erscheinen unserer Einschätzung nach willkürlich gewählt zu sein.
3. Die Prozessbeschreibung ist unvollständig.

Hinweis: Die gängigen Varianten der Prozesse der Datenträgervernichtung werden in der DIN SPEC 66399-3 umfassend beschrieben und Anforderungen definiert.

4. Der Anhang „A“ der EN 15713 entspricht nicht dem aktuellen Stand der Technik und ist aufgrund seines informativen Charakters kein verbindlicher Bestandteil der Norm.

Hinweis: Speziell die Definition der Spalte 2 „Mittlere Oberfläche des Materials in mm²“ ist äußerst kritisch zu sehen.

Im industriellen Zerkleinerungsbereich können, je nach eingesetzter Zerkleinerungstechnik, durchaus „Ausreißer“ nach oben entstehen (z.B. eine halbe DIN A4 Seite). Durch die Formulierung der EN 15713 kann das Ergebnis, durch den Anteil an kleinen und kleinsten Trümmerteilen (bis hin zu Staub), immer noch dem statistischen Mittelwert von XXXX mm², der in der Tabelle A.1 genannten Werte entsprechen.

Daher wird vom BSI empfohlen die EN 15713 nicht anzuwenden.

In der DIN 66399 und gleichlautend in der ISO/IEC 21964 wurde eine im Sinne der Sicherheit wesentlich bessere Formulierung gewählt. Hier wird, im Gegensatz zur EN 15713, im Fall der Materialteilchenoberfläche, von einem „maximal zulässigen“ Wert ausgegangen. Zwar gibt es

bei beiden Normen eine Toleranzmenge von 10 % der Gesamtmenge, die über der maximalen Materialteilchenfläche liegen darf, aber auch bei diesen 10 % gibt es eine exakte Beschränkung der maximalen Materialteilchenfläche nach oben.

3.4 DIN 32757

Die DIN 32757 wurde bereits 1985, und zwar ausschließlich als Norm, für die Hersteller für Schriftgutvernichter ins Leben gerufen.

Die DIN 32757 wurde mit Ausgabe der DIN 66399 im Jahre 2012 zurückgezogen.

4. Sicherheitskonzept

4.1 Sicherheitskonzept technische und organisatorische Maßnahmen

Sobald es darum geht, ein dem Risiko angemessenes Schutzniveau zu gewährleisten, müssen die technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen umgesetzt werden (vgl. Art. 32 Abs. 1 DS-GVO). Soweit es um DS-GVO-Compliance im Übrigen geht, sind demgegenüber die Berücksichtigung des Stands der Technik und der Implementierungskosten im Verhältnis zu dem durch diese Maßnahmen zu erreichenden Ziel nachrangig (vgl. unterbliebene Erwähnung in Art. 24 Abs. 1 Satz 1 DS-GVO).

Für den Vernichtungsprozess, der in der Regel arbeitsteilig organisiert ist (Behandlung des Materials innerhalb der Sphäre des Verantwortlichen und beim Vernichtungsdienstleister), muss das Sicherheitskonzept durchgängig und – was die Schutzbedürftigkeit der Daten betrifft – in sich schlüssig sein. Das Sicherheitskonzept wird regelmäßig im Hinblick auf die verschiedenen am Vernichtungsprozess Beteiligten aufgegliedert sein. Besonderes Augenmerk ist somit auf die Schnittstellen zwischen den Teilkonzeptionen zu legen. Hinweise für die Ausgestaltung des Sicherheitskonzepts können, in Abhängigkeit der gewählten Schutzklasse (vgl. vorstehende Ziff. 3.2.1.1) sowie der Variante (vgl. Ziff. 1.1), den in Abschnitt 6 enthaltenen Checklisten entnommen werden.

4.2 Zertifizierungen im Sinne des Datenschutzrechts

An dieser Stelle werden die für den Kunden bzw. Nutzer eines Vernichtungsdienstes bzw. -systems für Akten und Datenträger relevanten

Zertifizierungen im Sinne des Datenschutzrechts vorgestellt (d.h. im Sinne der Art. 42, 43 DS-GVO).

4.2.1 Grundlegendes

Die Mitgliedstaaten der EU, die für den Datenschutz zuständigen Aufsichtsbehörden, der Europäische Datenschutzausschuss und die EU-Kommission fördern die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen. Dies ist jedenfalls der erklärte Wille des europäischen Gesetzgebers, der in Art. 42 Abs. 1 Satz 1 DS-GVO niedergelegt wurde. Sowohl akkreditierte Zertifizierungsstellen als auch die zuständigen Aufsichtsbehörden können, nach Art. 42 Abs. 5 DS-GVO, eine solche Zertifizierung erteilen. Diese Art der Zertifizierung bietet die höchste Sicherheit im Hinblick auf die Datenschutzkonformität. Der Akkreditierungsprozess für den Bereich Datenschutz nach Art. 43 DS-GVO ist jedoch hinsichtlich seiner allgemeinen Ausgestaltung noch nicht mit allen Beteiligten final abgestimmt.

Im Detail verbergen sich jedoch Schwierigkeiten, die es gegenwärtig zumindest als fraglich erscheinen lassen, ob Zertifizierungen im Sinne der DS-GVO tatsächlich Marktbedürfnissen gerecht werden können. Die offene Frage ist, was genau zertifiziert werden kann (etwas Abstraktes oder nur etwas Konkretes)? Die Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen sollen dazu dienen, nachzuweisen, dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Diesen Wortlaut des Art. 42 Abs. 1 DS-GVO, der auf konkrete Verarbeitungstätigkeiten abstellt, wiederholt und vertieft Art. 42 Abs. 6 DS-GVO. Er ordnet an, dass der Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, Informationen zur Verfügung zu stellen hat. Die Bedürfnisse des Marktes verlangen jedoch nach abstrakten Zertifizierungen, wie sie ErwG 100 DS-GVO vor Augen hat. Solche Zertifizierungen treffen Aussagen über das Datenschutzniveau von Produkten und Dienstleistungen, notwendigerweise aufgrund einer abstrakten Betrachtung, die vom konkreten Einzelfall des Einsatzes eines Produktes bzw. der Ver-

wendung einer Dienstleistung losgelöst sind. Es bleibt abzuwarten und zu hoffen, dass die Aufsichtsbehörden die Art. 42, 43 DS-GVO so handhaben werden, wie es ErwG 100 DS-GVO vor Augen hat und wie es der Markt verlangt. Der Europäische Datenschutzausschuss veröffentlichte am 13.01.2019, nach abgeschlossener Konsultation der Öffentlichkeit, eine revidierte Fassung seiner „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679“. Bei Redaktionsschluss für diesen Leitfaden lagen jedoch noch keine praktischen Erfahrungen in der Anwendung dieser Richtlinien durch eine Aufsichtsbehörde vor.

4.2.2 Werbung mit Zertifizierungen

Soweit ein Dienstleister mit einem ihm erteilten Zertifikat, Testat, Prüfzeichen oder Ähnlichem wirbt und einen Bezug zwischen diesem und dem „Datenschutzrecht“ herstellt, sollten Auftraggeber diese Werbeaussage kritisch hinterfragen. Das Vorhandensein der Art. 42, 43 DS-GVO verbietet andere Zertifizierungen (und Ähnliches), die eine Konformität mit dem Datenschutzrecht attestieren wollen. Diese Aussage darf nur durch ein Zertifikat, Datenschutzsiegel oder -prüfzeichen formuliert werden, welches in Einklang mit den Art. 42 und 43 DS-GVO erteilt wurde. Welche Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen es jeweils aktuell europaweit gibt, lässt sich leicht und verbindlich nachprüfen, durch Einblick in das vom Europäischen Datenschutzausschuss geführte und gem. Art. 42 Abs. 8 DS-GVO veröffentlichte Register.

Alte Zertifikate, die aufgrund der von der Richtlinie 95/46/EG geprägten Rechtslage erteilt wurden (so insbesondere das Datenschutz-Gütesiegel vom ULD Schleswig-Holstein), wurden mit dem 25.05.2018 gegenstandslos. Einer jeden Aufsichtsbehörde steht es jedoch gem. Art. 42 Abs. 5 Satz 1 DS-GVO frei, in Zukunft Zertifikate i.S.v. Art. 42 DS-GVO zu erteilen. Ob eine oder mehrere deutsche Aufsichtsbehörden davon Gebrauch machen wollen, ist noch nicht entschieden.

Ungeachtet einer sich einstellenden regelmäßig geübten behördlichen Praxis, insbesondere geprägt durch die o.g. Richtlinien des Europäi-

schen Datenschutzausschusses, kann sich zukünftig der maßgebliche Rechtsrahmen ändern, ohne dass eine Änderung an der DS-GVO vorgenommen wird. Denn Art. 43 Abs. 9 DS-GVO ermächtigt die EU-Kommission, Durchführungsrechtsakte zu erlassen, mit denen technische Standards für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen sowie Mechanismen zur Förderung und Anerkennung dieser Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen festgelegt werden. Da diese Vorgaben gesetzlichen Rang haben, müssten sie von den Aufsichtsbehörden berücksichtigt und insoweit die behördliche Praxis erforderlichenfalls angepasst werden.

Um Datenschutzkonformität gegenüber dem Auftraggeber zu demonstrieren, kann zum aktuellen Zeitpunkt ein Testat zur Ermittlung des Umsetzungsgrades der DS-GVO anhand von selbst entwickelten Prüfkriterien einer Prüforganisation verwendet werden. Aufgrund der fehlenden Akkreditierung der Prüforganisation i.S.v. Art. 43 DS-GVO kann dieses Testat nur als (qualifizierte) Werbemaßnahme wahrgenommen werden. Um es zu vermeiden, dass Marktteilnehmer in die Irre geführt werden (unlauteres Wettbewerbsverhalten), ist jedoch darauf zu achten, dass durch das Testat bzw. die Art und Weise seiner werblichen Verwendung nicht der Eindruck einer Zertifizierung i.S.d. Art. 42, 43 DS-GVO erweckt wird. Zu empfehlen ist eine Testierung durch eine Prüforganisation allemal, da sie die inhaltliche Auseinandersetzung mit der DS-GVO bedingt und damit als gute Vorbereitung für eine spätere Zertifizierung durch eine akkreditierte Zertifizierungsstelle vorbereiten kann.

4.3 Zertifizierungen in Bezug auf technische Normen

Wenngleich mit einer anderen inhaltlichen Aussage als die Zertifizierungen im Sinne des Datenschutzrechts versehen, sind für den Kunden bzw. Nutzer eines Vernichtungsdienstes bzw. -systems für Akten und Datenträger auch Zertifizierungen in Bezug auf technische Normen wie jene der ISO, des DIN etc. von Interesse.

4.3.1 Grundlegendes

Der Verantwortliche i.S.v. Art. 4 Nr. 7 DS-GVO muss Gewissheit darüber haben, dass die Datenträgervernichtung, d.h. die zu erbringende Leistung „sach- und fachgerecht“ ausgeführt wird. Soweit Zertifizierungen in Bezug auf technische Normen Aussagen enthalten über die Qualität der Leistung des Auftragsverarbeiters, erhalten sie eine datenschutzrechtliche Relevanz. Denn Art. 28 Abs. 1 DS-GVO verlangt vom Auftraggeber eine Entscheidung über die Auswahl des Dienstleisters und erlegt ihm die Pflicht auf, den Auftrag nur einem solchen Dienstleister erteilen zu dürfen, der „hinreichend Garantien“ bietet. Garantien in diesem Sinne sind keine vertraglichen Zusagen, die garantiert werden, sondern Eigenschaften des Dienstleisters, einschließlich der Qualität der von ihm zu erbringenden Leistungen (vgl. ErwG 81 DS-GVO, der beispielhaft das Fachwissen, die Zuverlässigkeit und die Ressourcen des Dienstleisters nennt).

Die DIN 66399 Teil 2 sieht für Maschinen einen Prüfbericht und das Prüfzeugnis vor. Hierzu sieht die Norm einen Nachweis in der Bedienungsanleitung/Nutzerdokumentation vor, bei einigen Geräten finden sich auch Angaben auf dem Typenschild. Die Norm verlangt jedoch nur, dass das Prüfzeugnis „veröffentlicht“ werden muss. Der normale Kunde kann i.d.R. keinen für eine Maschine ausgestellten Prüfbericht verlangen.

Im Teil 3 der DIN 66399 wird für alle Prozessvarianten der Einsatz von Maschinen gemäß Teil 2 der Norm gefordert. Bei Einbindung eines Dienstleisters müssen sie sich zumindest das Prüfzeugnis der Maschine vorlegen lassen, im Zweifel darüber hinaus den Prüfbericht.

Die Einhaltung der Vorgaben an Dienstleister nach DIN 66399 Teil 3 sollte durch eine unabhängige Prüfstelle in einem Zertifikat bescheinigt sein. Ist die Prüfstelle ihrerseits durch eine unabhängige Akkreditierungsstelle anerkannt, so schafft dies zusätzliche Sicherheit.

Stärkt der 2. Teil der DIN 66399 auch die Transparenz bei der Prüfung von Maschinen, so enthält der 3. Teil erstmalig Prüflisten, die für eine Auditierung der einzelnen, während der Vernichtung zu beachtenden sowie umzusetzenden Prozessschritte nutzbar sind. Diese Listen wur-

den sowohl für die Vernichtung vor Ort durch die Unternehmen selbst, die mobile Vernichtung durch Dienstleister unmittelbar vor Ort als auch für die stationäre Vernichtung durch einen Dienstleister ausdifferenziert, um den unterschiedlichen Rahmenbedingungen der einzelnen Varianten Rechnung zu tragen. Wichtig sind allerdings auch die innerhalb der verschiedenen Varianten (siehe 1.1 Prozessbeschreibung) definierten normativen Vorgaben der DIN 66399, die ein Verantwortlicher selbst zu beachten hat.

Der Arbeitskreis empfiehlt, neben den Zertifikaten auch die zu Grunde liegenden Prüfberichte einzusehen, um eine Aussage darüber zu erhalten, ob die Dienstleistung ihren Anforderungen gerecht wird und die Prüfung (durch den Dritten) im gewünschten Umfang durchgeführt wurde.

Prüfzeugnisse für Maschinen werden manchmal als Zertifikat ausgestellt. Insbesondere bei Prüfungen durch unabhängige Prüfstellen empfehlen wir die vorgenannten Hinweise zu berücksichtigen.

4.3.2 Zertifizierung in Bezug auf andere Normen

Die Zertifizierungen der Anbieter nach den einschlägigen Normen ISO 14000 ff. (oder auch abfallwirtschaftlichen Normen, wie z.B. nach der Entsorgungsfachbetriebe-Verordnung (EfbV)) umfassen keine datenschutzrechtlichen Aspekte. Die daraus abzuleitenden Aussagen über die Qualität der Leistung oder die Eigenschaften des Dienstleisters sind in datenschutzrechtlicher Hinsicht irrelevant.

Anders verhält es sich mit Zertifizierungen der Anbieter nach Normen wie ISO 9000 ff. oder ISO 27000 ff., weil diese mittelbar für den Kunden bzw. Nutzer des Vernichtungsdienstes bzw. -systems für seine Auswahlentscheidung von Interesse sein können. So sollte sich z.B. ein beim Dienstleister effektiv etabliertes Qualitätsmanagementsystem mittelbar auf die Qualität der Leistung auswirken und eine Aussage über die Geschäftsorganisation des Dienstleisters (und damit über eine „hinreichende Garantie“ im Sinne einer Eigenschaft des Dienstleisters) enthalten.

4.4 Testate, Prüfberichte und Ähnliches von Wirtschaftsprüfern, Datenschutzbeauftragten u.a.

Bei einer Zertifizierung gibt es drei verschiedene Parteien: Den Auditierten, den Auditor und die Zertifizierungsstelle. Der Auditbericht des von der Zertifizierungsstelle akkreditierten Auditors, wird zur Überprüfung an die Zertifizierungsstelle geschickt. Wenn dieser den Regularien der Zertifizierung entspricht, wird von der Zertifizierungsstelle ein entsprechendes Zertifikat erteilt. Die Beteiligung dieser drei Parteien soll die Qualität und Vergleichbarkeit der Zertifikate gewährleisten. Zudem verhindert oder erschwert ein solches Vorgehen "Gefälligkeits-Zertifikate".

4.4.1 Grundlegendes

Bei der Testierung gibt es demgegenüber nur zwei Parteien: Den Auditierten und den Auditor. Damit entfallen die vorgenannten Vorteilte der Zertifizierung. Ferner wird der Auditor regelmäßig vom Auditierten mit der Prüfung bzw. Testierung beauftragt und von ihm bezahlt. Somit besteht eine Abhängigkeit des Auditors vom Auditierten, die Gefahren in sich birgt. Soweit bisweilen sogar interne Datenschutzbeauftragte des Dienstleisters als „unabhängige Instanzen“ gesehen wurden, sollte den von ihnen ausgestellten Testaten, Prüfberichten und ähnlichen Dokumenten, soweit diese vom Dienstleister offensiv kommuniziert bzw. zur Werbung eingesetzt werden, von Seiten der Auftraggeber angemessen skeptisch begegnet werden.

Ob externe Prüfer generell unabhängiger sind und dadurch die Vermutung einer höheren Qualität der Prüfung für sich beanspruchen können, im Vergleich zu Prüfungen durch Arbeitnehmer, ist eine Einzelfallfrage. Soweit die Aussage pauschal formuliert wird, ist ihr entgegenzutreten. Die wirtschaftliche Abhängigkeit des Auditors vom Auditierten kann bei externen Prüfern viel gravierendere Auswirkungen haben, als sie sich bei einem – mit besonderem Kündigungsschutz ausgestatteten – Arbeitnehmer einstellen.

Ein wesentlicher Nachteil im Vergleich zu o.g. Zertifizierungen ist, dass es den Testaten, Prüfberichten und Ähnlichem an einem verbindlichen Prüfungsmaßstab bzw. einer verbindlichen Vorgabe des Prüfungsgenstandes (Scope) fehlt. Während o.g. Zertifikate mit Blick auf das Gesetz oder eine technische Norm ausgestellt werden und daher einen vorgegebenen Prüfungsmaßstab betrachten, obliegt es im Bereich der rechtlich ungeschützten Begriffe „Testate“ etc. dem Inhalt der entgeltlichen Beauftragung, den Prüfungsgegenstand und Prüfungsmaßstab zu definieren. Insoweit ist insbesondere bei reißerisch formulierten Prüfungsergebnissen, die insbesondere an der bloßen Verwendung von Schlagworten und der Benutzung von Superlativen zu erkennen sind, eine kritische Distanz zum Ergebnis geboten.

4.4.2 Werbung mit den Ergebnissen der Prüfung von Wirtschaftsprüfern

Einige Dienstleister im Bereich der Akten- und Datenträgervernichtung sind gesetzlich verpflichtet, eine Jahresabschlussprüfung durch Wirtschaftsprüfer durchführen zu lassen. Ein nicht geringer Teil davon beinhaltet eine Prüfung der informationstechnischen Systeme, die für die Buchhaltung und Erstellung des Jahresabschlusses relevant sind.

Dieser Teil wird immer umfangreicher und kann relativ einfach auf informationstechnische Systeme ausgedehnt werden, die die Dienstleister für ihr Kerngeschäft, d.h. die Leistungserbringung gegenüber dem Auftraggeber einsetzen. Auftraggeber sollten bei Werbeaussagen mit Prüfberichten von Wirtschaftsprüfern berücksichtigen, dass es das Ziel einer Abschlussprüfung ist, (lediglich) mit hinreichender Sicherheit zu beurteilen, ob bei der Erstellung des zu prüfenden Abschlusses sämtliche relevanten Rechnungslegungsnormen beachtet wurden. Es sollte bekannt sein, dass Abschlussprüfungen stets ein risikoorientierter Prüfungsansatz zu Grunde liegt, d.h. keine Vollprüfung des Prüfungsgegenstands vorgenommen wird. Insoweit muss eindringlich vor einer Verwechslungsgefahr gewarnt werden: Der „risikoorientierte“ Ansatz der DS-GVO, der seinen Niederschlag in den Art. 32 bis 36 DS-GVO gefunden hat (und schon seinerseits mit DS-GVO-Compliance im Übrigen

nichts zu tun hat, vgl. Zwecke der Maßnahmen in Art. 24 Abs. 1 und Art. 32 Abs. 1 DS-GVO), hat mit einem „risikoorientierten Prüfungsansatz“ (d.h. einer bewusst lückenhaften Prüfung) nichts gemein. Ferner muss bedacht werden, dass explizit nicht die Aufgabe eines Wirtschaftsprüfers ist, ein Urteil über die wirtschaftliche Lage eines Unternehmens abzugeben und erst recht nicht (schon mangels Qualifikation, vgl. § 4 WiPrPrüfV) ein Urteil über die (datenschutz-)rechtliche Lage eines Unternehmens abzugeben.

Dies ist insbesondere zu betonen, für die von Wirtschaftsprüfern offerierten „Prüfungen informationstechnischer Systeme außerhalb der Abschlussprüfung“, entsprechend dem vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) formulierten Prüfungsstandard IDW PS 860, soweit durch den Wirtschaftsprüfer unter Berufung auf die IDW Prüfungshinweise IDW-PH-9/860/1 Aussagen zum Datenschutzrecht formuliert werden. Ausweislich der Vorbemerkung beanspruchen die IDW-PH-9/860/1 für sich die Funktion, die zwecks „Prüfung nach der EU-Datenschutz-Grundverordnung (DS-GVO) und dem BDSG“ zu Grunde zu legenden Kriterien zu „konkretisieren“. Mangels der von einer zuständigen Aufsichtsbehörde oder der EU-Kommission erteilten Genehmigung für die IDW-PH-9/860/1 i.S.v. Art. 40 Abs. 6, Abs. 9 DS-GVO sind die Prüfungshinweise jedoch nicht in der Lage, wirksam eine Konkretisierung von gesetzlichen Anforderungen vorzunehmen. Mangels Betrachtung eines homogenen Sachverhalts i.S.v. Art. 40 Abs. 2 DS-GVO sind sie auch nicht genehmigungsfähig. Der oben erteilte Hinweis auf die Irreführung des Marktes, die bei „Zertifizierungen des Datenschutzes“ droht, welche nicht den Regelungen der Art. 42, 43 DS-GVO folgen, gilt entsprechend auch für jeden Versuch, gesetzliche Anforderungen zu konkretisieren, sofern nicht die Vorgaben der Art. 40, 41 DS-GVO beachtet werden. Denn für diesen Zweck, Konkretisierung des abstrakten Gesetzes im Hinblick auf bestimmte homogene Sachverhalte, schuf der Gesetzgeber das Instrument der Verhaltensregeln. Auch in Bezug darauf haben kreative Ideen der freien Marktwirtschaft ein Abstandsgebot zu beachten, um den Vorwurf der Irreführung zu vermeiden.

Hingegen sollten von Auftraggebern die Prüfungen von Systemen der Dienstleister, die für die Leistung der Akten- und Datenträgervernich-

tung nur mittelbar bzw. indirekt relevant sind, nicht übersehen werden. Wie bereits zu Beginn dieses Ratgebers formuliert, favorisiert der Arbeitskreis „Sicherheit durch Qualität“. Zu den dort angesprochenen Sicherheits- und Kontrollsystemen gehören auch interne Kontrollsysteme (IKS). Insoweit seien die Auftraggeber darauf aufmerksam gemacht, dass es auch dienstleistungsbezogene Kontrollsysteme gibt, die einer Auditierung durch Wirtschaftsprüfer auf Basis des Prüfstandards IDW PS 951 zugänglich sind (dieser bezieht sich auf die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen; siehe dazu oben, Abschnitt 2.3).

5. FAQ/Handlungsempfehlungen

5.1 Auslegung der Schutzklasse 3

Bei Vernichtung von Datenträgern durch Dienstleister entsprechend der Vorgaben an Prozesse nach DIN SPEC 66399 Teil 3 / ISO 21964 Teil 3 (siehe auch Maßnahme V3.72) macht die Norm zum Prozessschritt Vernichtung folgende Vorgabe:

„Das Bedienpersonal darf grundsätzlich keinen Zugriff auf zu vernichtende Datenträger in Originalgröße (DIN66399-2 Kategorie P) haben. Der Maschine zur Vernichtung der Datenträger wird der Inhalt der eingesetzten Sicherheitsbehälter entweder direkt oder über eine entsprechend gesicherte Zuführeinrichtung zugeführt."

Der Normenausschuss hat diese Anforderung gestellt, um im Vernichtungsprozess den absichtlichen oder zufälligen Zugriff auf Akten/Dokumente prinzipiell auszuschließen und im Ausnahmefall auf das gebotene Minimum zu beschränken. Die Forderung „grundsätzlich keinen Zugriff" ist so zu verstehen, dass die Zugriffsmöglichkeit sowohl im normalen Ablauf der Vernichtung als auch durch konstruktive Maßnahmen der Anlage verhindert ist. Insofern genügt das Abkippen von Datenträgern in einen Sammelbunker, z.B. beim Einsatz von Großbehältern (Absetz- oder Abrollmulden) oder die Möglichkeit zur manuellen Sortierung den an die Vernichtung von Informationsträgern der Schutzklasse 3 gestellten Anforderungen nicht. Denn hier ist schon aufgrund der technischen Auslegung die Möglichkeit gegeben, dass Datenträger im Bereich verbleiben und im normalen Ablauf regelmäßig, teilweise von Hand entfernt werden müssen.

Vorgesehen war die Regelung „grundsätzlich" für Störungen an der Vernichtungsmaschine selbst oder der Zuführeinrichtung der Sicherheitsbehälter, oder z.B. im Brandfalle.

Insofern hat der Auftraggeber zu kontrollieren, dass die normative Vorgabe dieses Erfordernisses vom Dienstleister in seiner Umsetzung des Gesamtprozesses wirkungsvoll erreicht wird.

5.2 Berücksichtigung ökologischer Aspekte

Zum Vernichten von Datenträgern unter Berücksichtigung ökologischer und ökonomischer Aspekte (DIN 66399 Teil 1, Kap. 5.1) bzw. DIN 66399 Teil 2 am Beispiel von Festplatten:

Bei Festplatten mit magnetischem Datenträger ist nur die Vernichtung der „Scheiben“ der Festplatte notwendig. Um den Aufwand bei der Vernichtung zu minimieren sollten diese vor der Vernichtung, insbesondere bei hohen Sicherheitsstufen, vorab zerlegt werden. Alle anderen Teile können dem Recyclingprozess zugeführt werden. Bei der Beurteilung der Vernichtungsqualität sind zudem Gehäuseteile nicht relevant. Diese dürfen die normativen Vorgaben an die Partikelgröße überschreiten, wenn sichergestellt ist, dass die eigentlichen Datenträger (Scheiben) entsprechend vernichtet werden.

5.3 Berücksichtigung der Größe eines Datenträgers

Zum Vernichten von elektronischen Datenträgern:

In den Sicherheitsstufen E-5 und höher wird neben der Partikelgröße gefordert, dass der Datenträger (Chip) mehrfach zerteilt ist. Chips moderner Chipkarten sind oft erheblich kleiner als die in Sicherheitsstufe E-5 geforderten 10 mm². Ein Zerteilen mit Maschinen, die die Anforderungen der Sicherheitsstufe E-5 an sich erfüllen, kann den Vorgaben der Norm insgesamt nicht gerecht werden. In solchen Fällen ist eine höhere Sicherheitsstufe auszuwählen, vgl. DIN 66399-1 Kap. 5.1.

5.4 Einsatz von Verbrennungsanlagen

Die DIN 66399-2 sieht für Datenträger mit dem Schutzbedarf der Schutzklasse 3, insbesondere für die Sicherheitsstufen 6 und 7 sehr hohe Anforderungen bezüglich der zu erzielende Partikelgrößen vor, welche mit herkömmlichen Großanlagen (Desintegratoren), Schredder oder Schneidmühlen nur mit extrem hohem Aufwand zu erzielen sind. Die Norm sieht vor, dass die Sicherheitsstufen auch dadurch zu erreicht

werden können, dass die Datenträger zu Asche zerkleinert, aufgelöst oder auch geschmolzen werden (Sicherheitsstufen P7, F6, F7, O6, O7, T7, H7, E6 und E7). Dies bedeutet jedoch nicht, dass die Datenträger ohne vorherige Zerkleinerung oder nach einer groben Vorzerkleinerung ohne weitere Voraussetzungen oder Maßnahmen zu der Verbrennungsanlage transportiert und dort weiterverarbeitet werden können. Die ist aus prozesstechnischen Gründen oft gefordert. Darüber hinaus schafft die Vorzerkleinerung bereits einen Basisschutz im Gesamtprozess, z.B. für Risiken beim Transport zur weiteren Vernichtung entsprechend der geforderten Sicherheitsstufe.

Wie weiter oben ausgeführt wird, ist die Datenträgervernichtung als ein ganzheitlicher Prozess, von der Sammlung beim Verantwortlichen bis zur Vernichtung, zu verstehen.

Da der Prozess erst mit der auftragskonformen Vernichtung als abgeschlossen gilt, müssen auch sämtliche Prozesskriterien der DIN 66399 über den gesamten Prozessablauf eingehalten werden. Folgerichtig ist die Verbrennungsanlage, entweder als Auftragnehmer selbst oder als Unterauftragnehmer, als ein Auftragsverarbeiter zu qualifizieren, welcher ebenfalls hinreichende Garantien i.S.v. ErwGr 81 DS-GVO bieten können muss und für dessen Einsatz ein Vertrag mit dem gebotenen Mindestinhalt erforderlich ist (vgl. vorstehende Ziff. 2.1.2).

5.5 Erläuterung der Begriffe Entsorgung und Vernichtung

Die Begriffe Entsorgung und Vernichtung werden häufig im gleichen Kontext verwendet. In ihrer Bedeutung unterscheiden diese sich jedoch wesentlich.

Die Entsorgung berücksichtigt lediglich die Aspekte aus den einschlägigen gesetzlichen Vorgaben wie KrWG, ElektroG usw. Dem Schutzbedarf der Daten wird in diesen Prozessen gar nicht oder eher zufällig Rechnung getragen.

Erst das Vernichten der Daten/Datenträger mit der durch den Verantwortlichen festgelegten Schutzklasse und Sicherheitsstufe in einem

sicheren Gesamtprozess soll zur Einhaltung der gesetzlichen Vorgaben (u.a. DS-GVO, SÜG, ...) führen.

5.6 Vorgehensweise zu verschlüsselten Datenträgern

Nach dem Stand der Technik verschlüsselte Datenträger sollen nur nach vollständigem Überschreiben des Datenträgers einer Entsorgung zugeführt werden.

Besteht Unklarheit über den Zustand eines (verschlüsselten) Datenträgers, z.B. durch Defekt oder mangelhafte Funktion, wird eine Vernichtung empfohlen.

5.7 Zur normativen Anforderung an Sicherheitsbehältern

Die DIN66399 / ISO 21964 fordert für Variante 2 und 3 dem Schutzbedarf angemessene geschlossene und verschlossene Sicherheitsbehälter einzusetzen. Die Sicherheitsbehälter sind, bis auf eine Einwurföffnung, auf allen Seiten geschlossene Behälter zu verstehen, die keine Einsichtnahme oder Entnahme des enthaltenen Materials erlauben und die Schlossfalle eingerastet ist.

Die Anforderung "verschlossen" bedeutet nach dem Stand der Technik, dass das verwendete Schloss den geschlossenen Behälter mit einem Riegel sichert.

Gängige Sicherheitsbehälter verwenden oft sogenannte Fallenschlösser. Diese erfüllen die normativen Anforderungen an den Verschluss dann, wenn durch organisatorische Maßnahmen im Gesamtprozess ein unberechtigter Zugriff auf den Behälter durch Unbefugte wirkungsvoll unterbunden wird. So sollen solche Behälter nicht in Räumlichkeiten/Bereichen aufgestellt oder aufbewahrt werden, die unbemerkt durch unbefugte Personen betreten werden können (z.B. freier Zugang mit Publikumsverkehr).“

6. Checkliste

6.1 Variante 1 (Datenträgervernichtung durch den Verantwortlichen direkt)

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
Organisation und Personal				
V1.1	Beim Verantwortlichen ist ein/e Verantwortliche/r für die Vernichtung von Datenträgern benannt und den Beschäftigten bekannt.	möglich	erforderlich	erforderlich
V1.2	Die Erforderlichkeit eines Datenschutzbeauftragten ist gegeben und dieser ist vom Verantwortlichen benannt.	erforderlich	erforderlich	erforderlich
V1.3	Vor dem Hintergrund datenschutzrelevanter und wirtschaftlicher (kritische Unternehmensdaten) Aspekte ist ein Schutzniveau in Bezug auf Vernichtung von Daten definiert (Schutzklassen).	erforderlich	erforderlich	erforderlich
V1.4	Die Vernichtungsprozesse von/für personenbezogene Daten sind im Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen aufgeführt.	erforderlich	erforderlich	erforderlich
V1.5	Die definierten Vernichtungsprozesse umfassen sämtliche Materialkategorien (P, F, O, T, H, E), auf denen unternehmens- und/oder personenbezogene Daten gespeichert werden.	erforderlich	erforderlich	erforderlich
V1.6	Es liegt eine Dokumentation der Vernichtungsprozesse unter Berücksichtigung aller eingesetzten Materialkategorien vor.	erforderlich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V1.7	Unternehmensinterne Zuständigkeiten/Verantwortlichkeiten für Zwischenfälle/besondere Vorkommnisse in Bezug auf die Vernichtung von Datenträgern sind definiert.	erforderlich	erforderlich	erforderlich
V1.8	Es existiert eine Organisationsrichtlinie (Dienstanweisung) zur Datenträgervernichtung.	erforderlich	erforderlich	erforderlich
V1.9	Verantwortlichkeiten sind in dieser Richtlinie eindeutig definiert.	erforderlich	erforderlich	erforderlich
V1.10	Bei Verstoß gegen diese Richtlinie sind Sanktionen/Eskalationsstufen festgelegt.	erforderlich	erforderlich	erforderlich
V1.11	Das eigene Personal ist im Umgang mit zu vernichtendem Material geschult und unterwiesen.	erforderlich	erforderlich	erforderlich
V1.12	Die Richtlinie ist den Mitarbeitern bekannt und wird eingehalten.	erforderlich	erforderlich	erforderlich
V1.13	Die Richtlinie umfasst alle zur Vernichtung anfallenden Materialkategorien.	erforderlich	erforderlich	erforderlich
V1.14	Festlegung der Sicherheitsstufe in Abhängigkeit des Schutzbedarfs nach DIN 66399-1.	erforderlich	erforderlich	erforderlich
V1.15	Es sind technische und organisatorische Maßnahmen für den Vernichtungsprozess (Anfallstelle, Sammlung, Lagerung und Vernichtung) zu definieren.	erforderlich	erforderlich	erforderlich
V1.16	Die aufbewahrenden Stellen für Schlüsselsysteme (Räume/Behälter) sind durch den Verantwortlichen legitimiert.	möglich	erforderlich	erforderlich
V1.17	Es gibt ein Konzept für Havarien im Prozess (Transport/Vernichtungsanlage).	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V1.18	Alle am Prozess beteiligten Personen und Dritte, sofern deren Zugriff auf die Datenträger oder Kenntnisnahme von Daten nicht ausgeschlossen werden kann, sind auf die Vertraulichkeit verpflichtet (z.B. Wartungstechniker).	erforderlich	erforderlich	erforderlich
Anfallstelle zur Datenträgervernichtung				
V1.19	Das Erfassungs-/Vernichtungssystem ist so aufgestellt, dass eine Integration der Datenträgervernichtung in das Tagesgeschäft möglichst einfach ist.	erforderlich	erforderlich	erforderlich
V1.20	Der Bereich der Datenträgervernichtung ist eindeutig von anderen Geschäftsbereichen des Unternehmens getrennt (z.B. Altpapierentsorgung).	möglich	erforderlich	erforderlich
V1.21	Alternative (unsichere) Entsorgungswege (Papierkorb, etc.) sind organisatorisch untersagt.	möglich	erforderlich	erforderlich
V1.22	Es erfolgt eine Vernichtung oder Vorbehandlung von Medien am Entstehungsort unter Berücksichtigung/Vorgabe der Richtlinie zur Vernichtung von Datenträgern.	erforderlich	erforderlich	erforderlich
V1.23	Eine Zutrittskontrolle (Gebäude, Büro, Ort der Vernichtung etc.) ist gewährleistet.	möglich	erforderlich	erforderlich
V1.24	Die interne Weitergabe/Übergabe von zu vernichtenden Datenträgern (z.B. erzeugende Abteilung an mit Vernichtung betraute Abteilung) wird dokumentiert.	möglich	erforderlich	erforderlich
V1.25	Die mit Sammlungs- und Transportaufgaben betrauten internen Mitarbeiter sind als solche bekannt (Regelungen für das Ausscheiden der Mitarbeiter!).	erforderlich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V1.26	Im Sicherheitsbereich ist eine Videoüberwachung mit Aufzeichnung oder ein Behälterverfolgungssystem vorhanden.	möglich	möglich	erforderlich
V1.27	Eine Alarmanlage bzw. ein Wachdienstsystem ist umgesetzt.	möglich	möglich	erforderlich
Sammeln gegebenenfalls Lagern				
V1.28	Das zu vernichtende Material wird nach Dienstschluss in verschlossenen Räumen (Entstehungsort) aufbewahrt.	möglich	erforderlich	erforderlich
V1.29	Das zu vernichtende Material wird nach Dienstschluss in verschlossenen Behältern (Entstehungsort) aufbewahrt.	möglich	möglich	erforderlich
V1.30	Datenschutzrelevante Datenträger werden grundsätzlich zugriffssicher aufbewahrt.	möglich	erforderlich	erforderlich
V1.31	Sammelstellen für zu vernichtende Datenträger sind durch eine eindeutige Kennung identifiziert und in einem zentralen Verzeichnis dokumentiert.	möglich	erforderlich	erforderlich
V1.32	Es sind Zutrittsregelungen zu Räumlichkeiten zur Sammlung/Zwischenlagerung von zu vernichtenden Datenträgern vorhanden.	möglich	erforderlich	erforderlich
V1.33	Der Zutritt durch Betriebsfremde zum Bereich in dem gesammelt bzw. zwischengelagert wird, ist ohne Legitimation ausgeschlossen.	erforderlich	erforderlich	erforderlich
Datenträgervernichtung direkt				
V1.34	Einsatz von Maschinen zur Vernichtung von Datenträgern nach DIN 66399-2.	erforderlich	erforderlich	erforderlich
V1.35	Der Verantwortliche muss die ordnungsgemäße Vernichtung durch regelmäßige Probenahme kontrollieren.	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V1.36	Ein Nachweis ist zu erbringen, dass geeignete Maschinen für die zu vernichtenden Datenträgerkategorien verwendet werden.	erforderlich	erforderlich	erforderlich

6.2 Variante 2 (Datenträgervernichtung vor Ort durch Dienstleister)

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
Organisation und Personal				
V2.1	Beim Verantwortlichen ist eine Person für die Vernichtung von Datenträgern benannt und den Beschäftigten bekannt.	möglich	erforderlich	erforderlich
V2.2	Die Erforderlichkeit eines Datenschutzbeauftragten ist gegeben und dieser ist vom Verantwortlichen benannt.	erforderlich	erforderlich	erforderlich
V2.3	Vor dem Hintergrund datenschutzrelevanter und wirtschaftlicher (kritische Unternehmensdaten) Aspekte ist ein Schutzniveau in Bezug auf Vernichtung von Daten definiert (Schutzklassen).	erforderlich	erforderlich	erforderlich
V2.4	Die Vernichtungsprozesse von/für personenbezogene Daten sind im Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen aufgeführt.	erforderlich	erforderlich	erforderlich
V2.5	Die definierten Vernichtungsprozesse umfassen sämtliche Materialkategorien (P, F, O, T, H, E), auf denen unternehmens- und/oder personenbezogene Daten gespeichert werden.	erforderlich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V2.6	Es liegt eine Dokumentation der Vernichtungsprozesse unter Berücksichtigung aller eingesetzten Materialkategorien vor.	erforderlich	erforderlich	erforderlich
V2.7	Unternehmensinterne Zuständigkeiten/Verantwortlichkeiten für Zwischenfälle/besondere Vorkommnisse in Bezug auf die Vernichtung von Datenträgern sind definiert.	erforderlich	erforderlich	erforderlich
V2.8	Es existiert eine Organisationsrichtlinie (Dienstanweisung) zur Datenträgervernichtung.	erforderlich	erforderlich	erforderlich
V2.9	Verantwortlichkeiten sind in dieser Richtlinie eindeutig definiert.	erforderlich	erforderlich	erforderlich
V2.10	Bei Verstoß gegen diese Richtlinie sind Sanktionen/ Eskalationsstufen festgelegt.	erforderlich	erforderlich	erforderlich
V2.11	Das eigene Personal ist im Umgang mit zu vernichtendem Material geschult und unterwiesen.	erforderlich	erforderlich	erforderlich
V2.12	Die Richtlinie ist den Mitarbeitern bekannt und wird eingehalten.	erforderlich	erforderlich	erforderlich
V2.13	Die Richtlinie umfasst alle zur Vernichtung anfallenden Materialkategorien.	erforderlich	erforderlich	erforderlich
V2.14	Festlegung der Sicherheitsstufe in Abhängigkeit des Schutzbedarfs nach DIN 66399-1.	erforderlich	erforderlich	erforderlich
V2.15	Es sind technische und organisatorische Maßnahmen für den Vernichtungsprozess (Anfallstelle, Sammlung, Lagerung, Transport, Vernichtung) definiert. Der Verantwortliche legt fest, welche Prozessabschnitte und Aufgaben der Dienstleister im Vernichtungsprozess übernimmt.	erforderlich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V2.16	Die aufbewahrenden Stellen für Schlüsselsysteme (Räume/Behälter) sind durch den Verantwortlichen legitimiert.	möglich	erforderlich	erforderlich
V2.17	Alle am Prozess beteiligten Personen und Dritte, sofern deren Zugriff auf die Datenträger oder Kenntnisnahme von Daten nicht ausgeschlossen werden kann, sind auf die Vertraulichkeit verpflichtet (z.B. Wartungstechniker).	erforderlich	erforderlich	erforderlich
Anfallstelle zur Datenträgervernichtung				
V2.18	Das Erfassungs- und Vernichtungssystem ist derart aufgestellt, dass eine Integration der Datenträgervernichtung in das Tagesgeschäft möglichst einfach ist.	erforderlich	erforderlich	erforderlich
V2.19	Der Bereich der Datenträgervernichtung ist eindeutig von anderen Geschäftsbereichen des Unternehmens getrennt (z.B. Altpapierentsorgung).	möglich	erforderlich	erforderlich
V2.20	Alternative (unsichere) Entsorgungswege (Papierkorb, etc.) sind organisatorisch untersagt.	möglich	erforderlich	erforderlich
V2.21	Es erfolgt eine Vernichtung oder Vorbehandlung von Medien am Entstehungsort unter Berücksichtigung/Vorgabe der Richtlinie zur Vernichtung von Datenträgern.	erforderlich	erforderlich	erforderlich
V2.22	Eine Zutrittskontrolle (Gebäude, Büro, Ort der Vernichtung etc.) ist gewährleistet.	möglich	erforderlich	erforderlich
V2.23	Die interne Weitergabe/Übergabe von zu vernichtenden Datenträgern (z.B. erzeugende Abteilung an mit Vernichtung betraute Abteilung) wird dokumentiert.	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V2.24	Die mit Sammlungs- und Transportaufgaben betrauten internen Mitarbeiter sind als solche bekannt (Regelungen für das Ausscheiden der Mitarbeiter).	erforderlich	erforderlich	erforderlich
Sammeln gegebenenfalls Lagern				
V2.25	Das zu vernichtende Material wird nach Dienstschluss in verschlossenen Räumen (Entstehungsort) aufbewahrt.	möglich	erforderlich	erforderlich
V2.26	Das zu vernichtende Material wird nach Dienstschluss in verschlossenen Behältern (Entstehungsort) aufbewahrt.	möglich	möglich	erforderlich
V2.27	Datenschutzrelevante Datenträger werden grundsätzlich zugriffssicher aufbewahrt.	möglich	erforderlich	erforderlich
V2.28	Sammelstellen für zu vernichtende Datenträger sind durch eine eindeutige Kennung identifiziert und in einem zentralen Verzeichnis dokumentiert.	möglich	erforderlich	erforderlich
V2.29	Es sind Zutrittsregelungen zu Räumlichkeiten zur Sammlung/Zwischenlagerung von zu vernichtenden Datenträgern vorhanden.	möglich	erforderlich	erforderlich
V2.30	Der Zutritt durch Betriebsfremde zum Bereich in dem gesammelt bzw. zwischengelagert wird, ist ohne Legitimation ausgeschlossen.	erforderlich	erforderlich	erforderlich
V2.31	Es ist eindeutig geregelt wer für die jeweilige Anfallstelle die Abholung- bzw. Vernichtungsmeldungen aufgeben darf.	möglich	möglich	erforderlich
V2.32	Für die Sammlung, Lagerung und Transport von Datenträgern sind dem Schutzbedarf angemessene geschlossene und verschlossene Sicherheitsbehälter einzusetzen.	möglich	möglich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V2.33	Die Behälter sind derart gebaut, dass Fehlerquellen (z.B. Schließstörungen) durch die Verschlussart ausgeschlossen sind.	möglich	erforderlich	erforderlich
V2.34	Das Schließsystem ist geschützt und nur für den Inhaber des Behältersystems erhältlich.	möglich	erforderlich	erforderlich
V2.35	Die eingesetzte Schließanlage ist eine mind. 500er Schließanlage und ermöglicht diverse gleich schließende als auch verschieden schließende Behälterverschlusssysteme.	erforderlich	erforderlich	erforderlich
V2.36	Das Schließsystem ist derart ausgestaltet, dass eine Kopie von Schlüsseln oder sonstigen Schließungsinstrumentarien im Handel nicht möglich ist.	möglich	erforderlich	erforderlich
V2.37	Die Behältersysteme sind eindeutig durch z.B. Nummernfolge oder Barcode identifizierbar.	möglich	erforderlich	erforderlich
Transport vor Ort				
V2.38	Es sind Regelungen für die Übergabe der Datenträger an den intern Verantwortlichen bzw. den Dienstleister getroffen worden (intern: Arbeitsanweisung; extern: Vertrag gemäß Art. 28 DS-GVO).	möglich	erforderlich	erforderlich
V2.39	Die Übergabestelle und -form ist durch den Verantwortlichen legitimiert.	möglich	erforderlich	erforderlich
V2.40	Zum Transport sind dem Schutzniveau entsprechende Fahrzeuge zu verwenden.	erforderlich	erforderlich	erforderlich
V2.41	Die Mitarbeiter des Dienstleisters weisen sich durch Firmenausweise inkl. Lichtbild aus.	möglich	erforderlich	erforderlich
V2.42	Die Mitarbeiter sind durch Ihre Kleidung eindeutig dem eingesetzten Dienstleister zuzuordnen.	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V2.43	Der Fahrer besitzt eine genaue Arbeitsanweisung und Aufstellung der zu übernehmenden Behälter und einen zugehörigen Ansprechpartner beim Auftraggeber (Tel. Nr. und eventuell Kostenstelle).	möglich	erforderlich	erforderlich
Datenträgervernichtung Dienstleister vor Ort				
V2.44	Das Fahrzeug mit der Maschine zur Vernichtung der Datenträger muss über einen festen Aufbau verfügen.	erforderlich	erforderlich	erforderlich
V2.45	Einsatz von Maschinen zur Vernichtung von Datenträgern nach DIN 66399-2.	erforderlich	erforderlich	erforderlich
V2.46	Der Dienstleister ist für seinen Dienstleistungsprozess von einer unabhängigen und akkreditierten Stelle zertifiziert und unterliegt einer regelmäßigen Kontrolle.	möglich	erforderlich	erforderlich
V2.47	Es ist eine Vorabprüfung des Dienstleisters, insbesondere hinsichtlich des Niveaus der technisch-organisatorischen Maßnahmen vor Auftragsvergabe zusammen mit dem DSB durchgeführt worden.	möglich	erforderlich	erforderlich
V2.48	Es werden regelmäßig unangemeldete Kontrollen des Dienstleisters durch den Verantwortlichen durchgeführt.	möglich	erforderlich	erforderlich
V2.49	Die Überwachung aller Prozesse kann jederzeit und unangemeldet durch die Geschäftsführung des Unternehmens erfolgen (ohne Voranmeldung bzw. Warnzeiten).	erforderlich	erforderlich	erforderlich
V2.50	Sofern der Dienstleister Subauftragnehmer mit einbezieht, ist der Auftragnehmer darüber informiert und hat seine Zustimmung gegeben.	erforderlich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
	Diese sind ebenfalls gemäß den gestellten Anforderungen überprüft!)			
V2.51	Die Vernichtung erfolgt in Sicherheitsfahrzeugen, welche speziell für den Zweck der mobilen Datenträgervernichtung ausgestattet sind.	erforderlich	erforderlich	erforderlich
V2.52	Der Dienstleister/Verantwortliche muss die ordnungsgemäße Vernichtung durch regelmäßige Probenahme kontrollieren.	möglich	erforderlich	erforderlich
V2.53	Alle Mitarbeiter des Dienstleisters, die am Prozess beteiligt sind und Dritte, sofern deren Zugriff auf die Datenträger oder Kenntnisnahme von Daten nicht ausgeschlossen werden kann, sind auf die Vertraulichkeit verpflichtet (z.B. Wartungstechniker) wurden auf die Vertraulichkeit verpflichtet.	erforderlich	erforderlich	erforderlich
V2.54	Ein Nachweis ist zu erbringen, dass geeignete Maschinen für die zu vernichtenden Datenträgerkategorien verwendet werden.	erforderlich	erforderlich	erforderlich
V2.55	Der Dienstleister gestattet dem Verantwortlichen die Überwachung der Vernichtung der Datenträger.	möglich	erforderlich	erforderlich
V2.56	Es gibt ein Konzept für Havarien im Gesamtprozess der entsprechenden Prozessvariante.	möglich	erforderlich	erforderlich
V2.57	Redundanz und Verfügbarkeit der Vernichtungseinrichtung müssen über ein Notfallkonzept sichergestellt sein.	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung/ Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V2.58	Das Bedienpersonal darf grundsätzlich keinen Zugriff auf zu vernichtende Datenträger mit Informationsdarstellung in Originalgröße (DIN 66399-2 Kategorie P) haben. Der Maschine zur Vernichtung der Datenträger wird der Inhalt der eingesetzten Sicherheitsbehälter entweder direkt oder über eine entsprechend gesicherte Zuführeinrichtung zugeführt (vgl. Abschnitt 5.1).	möglich	möglich	erforderlich
V2.59	Videoüberwachung des Schüttvorgangs bzw. der Einfüllöffnung oder Zuführbandes der Maschine.	möglich	möglich	erforderlich
V2.60	Der Verantwortliche kann sich eine Probe seiner vernichteten Datenträger nehmen oder aushändigen zu lassen.	möglich	möglich	erforderlich

6.3 Variante 3 (Datenträgervernichtung extern durch Dienstleister)

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
Organisation und Personal				
V3.1	Beim Verantwortlichen ist ein/e Verantwortliche/r für die Vernichtung von Datenträgern benannt und den Beschäftigten bekannt.	möglich	erforderlich	erforderlich
V3.2	Die Erforderlichkeit eines Datenschutzbeauftragten ist gegeben und dieser ist vom Verantwortlichen benannt.	erforderlich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V3.3	Vor dem Hintergrund datenschutzrelevanter und wirtschaftlicher (kritische Unternehmensdaten) Aspekte ist ein Schutzniveau in Bezug auf Vernichtung von Daten definiert (Schutzklassen).	erforderlich	erforderlich	erforderlich
V3.4	Die Vernichtungsprozesse von/für personenbezogene/n Daten sind im Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen aufgeführt.	erforderlich	erforderlich	erforderlich
V3.5	Die definierten Vernichtungsprozesse umfassen sämtliche Materialkategorien (P, F, O, T, H, E), auf denen unternehmens- und/oder personenbezogene Daten gespeichert werden.	erforderlich	erforderlich	erforderlich
V3.6	Es liegt eine Dokumentation der Vernichtungsprozesse unter Berücksichtigung aller eingesetzten Materialkategorien vor.	erforderlich	erforderlich	erforderlich
V3.7	Unternehmensinterne Zuständigkeiten/Verantwortlichkeiten für Zwischenfälle/besondere Vorkommnisse in Bezug auf die Vernichtung von Datenträgern sind definiert.	erforderlich	erforderlich	erforderlich
V3.8	Es existiert eine Organisationsrichtlinie (Dienstanweisung) zur Datenträgervernichtung.	erforderlich	erforderlich	erforderlich
V3.9	Verantwortlichkeiten sind in dieser Richtlinie eindeutig definiert.	erforderlich	erforderlich	erforderlich
V3.10	Bei Verstoß gegen diese Richtlinie sind Sanktionen/ Eskalationsstufen festgelegt.	erforderlich	erforderlich	erforderlich
V3.11	Das eigene Personal ist im Umgang mit zu vernichtendem Material geschult und unterwiesen.	erforderlich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V3.12	Die Richtlinie ist den Mitarbeitern bekannt und wird eingehalten.	erforderlich	erforderlich	erforderlich
V3.13	Die Richtlinie umfasst alle zur Vernichtung anfallenden Materialkategorien.	erforderlich	erforderlich	erforderlich
V3.14	Festlegung der Sicherheitsstufe in Abhängigkeit des Schutzbedarfs nach DIN 66399-1.	erforderlich	erforderlich	erforderlich
V3.15	Es sind technische und organisatorische Maßnahmen für den Vernichtungsprozess (Anfallstelle, Sammlung, Lagerung, Transport, Vernichtung) definiert. Der Verantwortliche legt fest, welche Prozessabschnitte und Aufgaben der Dienstleister im Vernichtungsprozess übernimmt.	erforderlich	erforderlich	erforderlich
V3.16	Die aufbewahrenden Stellen für Schlüsselsysteme (Räume/Behälter) sind durch den Verantwortlichen legitimiert.	möglich	erforderlich	erforderlich
V3.17	Alle am Prozess beteiligten Personen und Dritte, sofern deren Zugriff auf die Datenträger oder Kenntnisnahme von Daten nicht ausgeschlossen werden kann, sind auf die Vertraulichkeit verpflichtet (z.B. Wartungstechniker).	erforderlich	erforderlich	erforderlich
Anfallstelle zur Datenträgervernichtung				
V3.18	Das Erfassungs- und Vernichtungssystem ist derart aufgestellt, dass eine Integration der Datenträgervernichtung in das Tagesgeschäft möglichst einfach ist.	erforderlich	erforderlich	erforderlich
V3.19	Der Bereich der Datenträgervernichtung ist eindeutig von anderen Geschäftsbereichen des Unternehmens getrennt (z.B. Altpapierentsorgung).	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V3.20	Alternative (unsichere) Entsorgungswege (Papierkorb, etc.) sind organisatorisch untersagt.	möglich	erforderlich	erforderlich
V3.21	Es erfolgt eine Vernichtung oder Vorbehandlung von Medien am Entstehungsort unter Berücksichtigung/Vorgabe der Richtlinie zur Vernichtung von Datenträgern.	erforderlich	erforderlich	erforderlich
V3.22	Eine Zutrittskontrolle (Gebäude, Büro, Ort der Vernichtung etc.) ist gewährleistet.	möglich	erforderlich	erforderlich
V3.23	Die interne Weitergabe/Übergabe von zu vernichtenden Datenträgern (z.B. erzeugende Abteilung an die mit der Vernichtung betraute Abteilung) wird dokumentiert.	möglich	erforderlich	erforderlich
V3.24	Die mit Sammlungs- und Transportaufgaben betrauten internen Mitarbeiter sind als solche bekannt. (Regelungen für das Ausscheiden der Mitarbeiter!)	erforderlich	erforderlich	erforderlich
Sammeln gegebenenfalls Lagern				
V3.25	Das zu vernichtende Material wird nach Dienstschluss in verschlossenen Räumen (Entstehungsort) aufbewahrt.	möglich	erforderlich	erforderlich
V3.26	Das zu vernichtende Material wird nach Dienstschluss in verschlossenen Behältern (Entstehungsort) aufbewahrt.	möglich	möglich	erforderlich
V3.27	Datenschutzrelevante Datenträger werden grundsätzlich zugriffssicher aufbewahrt.	möglich	erforderlich	erforderlich
V3.28	Sammelstellen für zu vernichtende Datenträger sind durch eine eindeutige Kennung identifiziert und in einem zentralen Verzeichnis dokumentiert.	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V3.29	Es sind Zutrittsregelungen zu Räumlichkeiten zur Sammlung/Zwischenlagerung von zu vernichtenden Datenträgern vorhanden.	möglich	erforderlich	erforderlich
V3.30	Der Zutritt durch Betriebsfremde zum Bereich in dem gesammelt bzw. zwischengelagert wird, ist ohne Legitimation ausgeschlossen.	erforderlich	erforderlich	erforderlich
V3.31	Es ist eindeutig geregelt wer für die jeweilige Anfallstelle die Abholung- bzw. Vernichtungsmeldungen aufgeben darf.	möglich	möglich	erforderlich
V3.32	Für die Sammlung, Lagerung und den Transport von Datenträgern sind dem Schutzbedarf angemessene geschlossene und verschlossene Sicherheitsbehälter einzusetzen.	möglich	möglich	erforderlich
V3.33	Die Behälter sind derart gebaut, dass Fehlerquellen (z.B. Schließstörungen) durch die Verschlussart ausgeschlossen sind.	möglich	erforderlich	erforderlich
V3.34	Das Schließsystem ist geschützt und nur für den Inhaber des Behältersystems erhältlich.	möglich	erforderlich	erforderlich
V3.35	Die eingesetzte Schließanlage ist eine mind. 500er Schließanlage und ermöglicht diverse gleich schließende als auch verschieden schließende Behälterverschlusssysteme.	erforderlich	erforderlich	erforderlich
V3.36	Das Schließsystem ist derart ausgestaltet, dass eine Kopie von Schlüsseln oder sonstigen Schließungsinstrumentarien im Handel nicht möglich ist.	möglich	erforderlich	erforderlich
V3.37	Die Behältersysteme sind eindeutig durch z.B. Nummernfolge oder Barcode identifizierbar.	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
Transport zum externen Dienstleister				
V3.38	Zum Transport sind dem Schutzniveau entsprechende Fahrzeuge zu verwenden.	erforderlich	erforderlich	erforderlich
V3.39	Das Fahrzeug verfügt über ein passives GPS-Ortungssystem oder der Transport ist durch mindestens 2 Personen zu begleiten.	möglich	erforderlich	erforderlich
V3.40	Es ist sichergestellt, dass die Fahrer oder Dritte während des Transports keinen Zugriff auf die in den Behältern enthaltenen Daten haben können (Schließsystem und Schlüsselverteilung).	möglich	erforderlich	erforderlich
V3.41	Es ist sichergestellt, dass die Behälter keine Zwischenlagerung oder eine Umladung erfahren und umgehend (taggleich) den Sicherheitsbereich des Dienstleisters erreichen.	möglich	erforderlich	erforderlich
V3.42	Die Übernahme der Datenträger bzw. Sicherheitsbehälter ist durch den Dienstleister in einem Übernahmeprotokoll zu dokumentieren.	erforderlich	erforderlich	erforderlich
V3.43	Der Dienstleister muss bei Verwendung von Umleerfahrzeugen und Vermischung von Datenträgern, die für die Vernichtung in unterschiedlichen Sicherheitsstufen vorgesehen sind, die höchste vereinbarte Sicherheitsstufe für die gesamte Ladung anwenden.	möglich	erforderlich	erforderlich
V3.44	Es sind Regelungen für die Übergabe der Datenträger an den intern Verantwortlichen bzw. den Dienstleister getroffen worden (intern: Arbeitsanweisung; extern: Vertrag gemäß Art. 28 DS-GVO).	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V3.45	Die Übergabestelle und -form ist durch den Verantwortlichen legitimiert.	möglich	erforderlich	erforderlich
V3.46	Sofern der Dienstleister den Subauftragnehmer mit einbezieht, ist der Auftragnehmer darüber informiert und hat seine Zustimmung gegeben. (Diese sind ebenfalls gemäß den gestellten Anforderungen überprüft!)	erforderlich	erforderlich	erforderlich
V3.47	Die Mitarbeiter des Dienstleisters weisen sich eindeutig durch Firmenausweise inkl. Lichtbild aus.	möglich	erforderlich	erforderlich
V3.48	Die Mitarbeiter sind durch ihre Kleidung eindeutig dem eingesetzten Dienstleister zuzuordnen.	möglich	erforderlich	erforderlich
V3.49	Der Fahrer besitzt eine genaue Arbeitsanweisung und Aufstellung der zu übernehmenden Behälter und einen zugehörigen Ansprechpartner beim Auftraggeber (Tel.-Nr. und eventuell Kostenstelle).	möglich	erforderlich	erforderlich
Sammeln gegebenenfalls Lagern				
V3.50	Alle am Prozess Beteiligten und alle Personen mit Zugang zur Sicherheitszone sind auf die Vertraulichkeit zu verpflichten (z.B. auch Wartungstechniker).	erforderlich	erforderlich	erforderlich
V3.51	Besucher oder Anlieferer werden während des Aufenthalts in der Sicherheitszone durch einen Mitarbeiter des Dienstleisters begleitet.	erforderlich	erforderlich	erforderlich
V3.52	Besucher werden mit einem Besucherausweis ausgestattet.	erforderlich	erforderlich	erforderlich
V3.53	Ein Umgang mit losen Datenträgern (z.B. Umladen, Umleeren) darf ausschließlich in einem geschlossenen Bereich erfolgen. Das Personal darf	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
	grundsätzlich keinen Zugriff auf zu vernichtende Datenträger mit Informationsdarstellung in Originalgröße (DIN 66399-2 Kategorie P) haben.			
V3.54	Die Lagerung (bis zur Vernichtung) und Entleerung der Sicherheitsbehälter findet ausschließlich innerhalb eines geschlossenen und überwachten Bereichs (Sicherheitszone) statt.	möglich	erforderlich	erforderlich
V3.55	Wenn unvernichtete Datenträger unbewacht gelagert werden, muss das Betriebsgebäude bzw. dieser Bereich mit einer Einbruchmeldeanlage ausgerüstet sein, welche zu einer Hilfe leistenden Stelle aufgeschaltet ist.	möglich	erforderlich	erforderlich
V3.56	Das Unternehmen besitzt ein Betriebsgebäude oder einen in sich geschlossenen Bereich (Sicherheitszone) in einem größeren Baukörper, welches/welcher ausschließlich zum Zwecke der Datenträgervernichtung genutzt wird.	erforderlich	erforderlich	erforderlich
V3.57	Das Betriebsgebäude bzw. der o. g. Bereich (Sicherheitszone) ist in massiver Bauausführung (z.B. Stahlbeton, massives Mauerwerk, mehrlagige Sandwich-Elemente) ausgeführt.	möglich	erforderlich	erforderlich
V3.58	Für die Einbringung von unvernichteten Datenträgern in die Sicherheitszone steht eine Schleuse oder dichte Andockstation (für Fahrzeuge) zur Verfügung.	möglich	erforderlich	erforderlich
V3.59	Alle Türen oder Tore, die direkt in die Sicherheitszone führen, schließen automatisch oder offene Türen/Tore werden durch optische oder akustische	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
	Meldeeinrichtungen angezeigt.			
V3.60	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.	möglich	erforderlich	erforderlich
V3.61	Die Sicherheitszone des Betriebsgebäudes wird durch Videokameras überwacht.	möglich	erforderlich	erforderlich
Datenträgervernichtung Dienstleister extern				
V3.62	Einsatz von Maschinen zur Vernichtung von Datenträgern nach DIN 66399-2.	erforderlich	erforderlich	erforderlich
V3.63	Der Dienstleister ist für seinen Dienstleistungsprozess von einer unabhängigen und akkreditierten Stelle zertifiziert und unterliegt einer regelmäßigen Kontrolle.	möglich	erforderlich	erforderlich
V3.64	Es ist eine Vorabprüfung des Dienstleisters, insb. hinsichtlich des Niveaus der technisch-organisatorischen Maßnahmen vor Auftragsvergabe zusammen mit dem DSB durchgeführt worden.	möglich	erforderlich	erforderlich
V3.65	Es werden regelmäßig unangemeldete Kontrollen des Dienstleisters durch den Verantwortlichen durchgeführt.	möglich	erforderlich	erforderlich
V3.66	Die Überwachung aller Prozesse kann jederzeit und unangemeldet durch die Geschäftsführung des Unternehmens erfolgen (ohne Voranmeldung bzw. Warnzeiten).	erforderlich	erforderlich	erforderlich
V3.67	Es gibt ein Konzept für Havarien im Gesamtprozess der entsprechenden Prozessvariante	möglich	erforderlich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V3.68	Die Verfügbarkeit der Maschine zur Vernichtung der Datenträger muss über ein Notfallkonzept sichergestellt sein.	möglich	erforderlich	erforderlich
V3.69	Der Dienstleister/Verantwortliche muss die ordnungsgemäße Vernichtung durch regelmäßige Probenahme kontrollieren.	möglich	erforderlich	erforderlich
V3.70	Ein Nachweis ist zu erbringen, dass geeignete Maschinen für die zu vernichtenden Datenträgerkategorien verwendet werden.	erforderlich	erforderlich	erforderlich
V3.71	Der Dienstleister gestattet dem Verantwortlichen die Überwachung der Vernichtung der Datenträger.	möglich	erforderlich	erforderlich
V3.72	Das Bedienpersonal darf grundsätzlich keinen Zugriff auf die zu vernichtenden Datenträger mit Informationsdarstellung in Originalgröße (DIN 66399-2 Kategorie P) haben. Der Maschine zur Vernichtung der Datenträger wird der Inhalt der eingesetzten Sicherheitsbehälter entweder direkt oder über eine entsprechend gesicherte Zuführeinrichtung zugeführt (vgl. Abschnitt 5.1).	möglich	möglich	erforderlich
V3.73	Videoüberwachung des Schüttvorgangs bzw. der Einfüllöffnung oder Zuführbandes der Maschine.	möglich	möglich	erforderlich
V3.74	Der Verantwortliche kann sich eine Probe seiner vernichteten Datenträger nehmen oder aushändigen lassen.	möglich	möglich	erforderlich
V3.75	Die Vernichtung erfolgt am Tag der Übernahme der zu vernichtenden Datenträger.	möglich	möglich	erforderlich

Kriterium	Maßnahmenempfehlung / Baustein	Erfüllung der Maßnahme für die Schutzklasse		
		1	2	3
V3.76	Redundanz der Maschine zur Vernichtung von Datenträgern muss vor Ort sichergestellt sein. Hinweis: Dies bedeutet nicht, dass eine zweite Maschine vor Ort vorgehalten werden muss. Es muss aber sichergestellt werden, dass bei Ausfall der Maschine taggleich die Vernichtung vor Ort erfolgen kann.	möglich	möglich	erforderlich

7. Begriffserläuterungen

Anfallstelle	Ort, an dem Datenträger aufbewahrt werden, um einer Vernichtung zugeführt zu werden
Auflösen	Überführen des Datenträgers in eine Suspension
Auftragsverarbeiter	Die Stelle i.S.v. Art. 4 Nr. 8 DS-GVO, d.h. eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
Datenträger	Objekt oder Gegenstand, der Daten enthält
Datenträgervernichtung	Vorgang, bei dem Form oder Zustand von Datenträgern in der Regel durch Zerkleinern, Auflösen, Schmelzen, Erhitzen oder Verbrennen verändert werden, wodurch die Wiederherstellung von Informationen erschwert oder unmöglich wird
Datenverarbeitung im Auftrag	Verarbeitungen von personenbezogenen Daten, die durch einen Auftragsverarbeiter im Auftrag eines Verantwortlichen ausgeführt werden; Auftrag ist der Vertrag oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, welcher bzw. welches die Bindung i.S.v. Art. 28 Abs. 3 Satz 1 DS-GVO erzeugt
Einbruchmeldeanlage	Alarmanlage zum Erkennen und Anzeigen der Anwesenheit, des Eindringens oder versuchten Eindringens eines Eindringlings in überwachte Objekte

Einrichtung	Zusammenstellung von in räumlichem und funktionalem Zusammenhang stehenden Maschinen zum Zweck der Datenträgervernichtung
Informationen	Daten, ungeachtet der Frage, ob diese personenbezogen sind oder nicht
Personenbezogene Daten	Daten i.S.v. Art. 4 Nr. 1 DS-GVO, d.h. alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
Regelmäßiger Partikel	Der Partikel weist auf Grund des verwendeten Schnittverfahrens eine üblicherweise unveränderbare, meist rechteckige Form sowie vorgegebene Breite und Länge auf
Schutzbedarf	Eigenschaft von Daten und Informationen, welche unter Berücksichtigung der bei einer Verletzung der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit zu erwartenden Schäden die Notwendigkeit beschreibt, diese Daten und Informationen vor einer Verletzung dieser Grundwerte zu bewahren
Schutzklasse	Klassifizierung des Schutzbedarfs von Daten
Schutzniveau	Definition nach BSI-Standard 100-2: normal, hoch, sehr hoch Nach der Bestimmung des zutreffenden Sicherheitsniveaus kann diese als Grundlage einer Schutzbedarfsfeststellung der Geschäftsprozesse dienen

Schutzzweck	Wahrung der Grundwerte der Informationssicherheit auf Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Im Entsorgungsprozess ist die Vertraulichkeit (Kenntnisnahme von Unbefugten) ein Schutzweck, dem ein ausreichendes Schutzniveau zugeordnet werden muss.
Sicherheitskonzept	Ein Sicherheitskonzept stellt im Allgemeinen eine Analyse möglicher Angriffs- und Schadenszenarien mit dem Ziel, ein definiertes Schutzniveau zu erreichen, dar. Unterschieden werden muss dabei die Sicherheit gegenüber böswilligen Angriffen (*Security*) und die Sicherheit gegenüber menschlichem und technischem Versagen (*Safety*).
Sicherheitsstufe	Klassifizierung des Aufwands zur Wiederherstellung von Informationen
Sicherheitszone	Entsprechend der Schutzklasse geschützter Bereich
Verantwortlicher	Die Stelle i.S.v. Art. 4 Nr. 7 DS-GVO, d.h. die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
Vernichtung	Vorgang, bei dem Form oder Zustand von Datenträgern in der Regel durch Zerkleinern, Auflösen, Schmelzen, Erhitzen oder Verbrennen verändert werden

8. Anlagen

8.1 Vertragsergänzung zur Auftragsverarbeitung

Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt

und

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Die Inhalte dieser Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag ergänzen die zwischen Auftraggeber und Auftragnehmer bestehenden bzw. gleichzeitig zu schließenden kaufmännischen Vereinbarungen, mithin den Auftrag i.S.v. Art. 28 DS-GVO, um die gesetzlich geforderten Mindestvertragsinhalte im Sinne von Art. 28 Abs. 3 DS-GVO. Die Parteien stellen klar, dass die kaufmännischen Vereinbarungen und diese Vereinbarung zur Auftragsverarbeitung einen einheitlichen Vertrag darstellen, auch wenn die Vertragsinhalte über verschiedene Dokumente verteilt sind. Mit dieser Vereinbarung wollen die Parteien sicherstellen, dass der Auftragnehmer seine Leistungen als

Auftragsverarbeiter erbringt, indem er im Sinne von Art. 28 Abs. 3 Satz 1 DS-GVO an den Auftraggeber gebunden wird.

1. Konkretisierung des Auftrags

1.1. Gegenstand der Verarbeitungstätigkeiten

Gegenstand der kaufmännischen Vereinbarungen ist die Erbringung von Leistungen der Akten- und Datenträgervernichtung durch den Auftragnehmer, die insbesondere die Übernahme und Vernichtung von Datenträgern gem. der bei Vertragsschluss gültigen Norm DIN 66399 umfassen. Die in den Akten und Datenträgern verkörperten personenbezogenen Daten sind infolgedessen Gegenstand der vertragsgegenständlichen Verarbeitungen.

1.2. Dauer der Verarbeitungstätigkeiten

Die Dauer der Verarbeitungstätigkeiten richtet sich nach den Festlegungen für die Leistung, die im Rahmen der kaufmännischen Vereinbarungen getroffen wurde.

1.3. Art(en) und Zweck(e) der vorgesehenen Verarbeitungstätigkeiten

Als Arten der Verarbeitung personenbezogener Daten durch den Auftragnehmer sind insbesondere das kurzzeitige Aufbewahren und das Löschen bzw. Vernichten vorgesehen, sowie etwaig ergänzende Tätigkeiten auf einzelfallbezogene Weisung des Auftraggebers. Der vom Auftraggeber verfolgte Zweck der Verarbeitungen, die er durch den Auftragnehmer ausführen lässt, ist das Löschen bzw. Vernichten der personenbezogenen Daten als solches.

1.4. Ort der Verarbeitungstätigkeiten

Die vertragsgegenständlichen Verarbeitungen finden ausschließlich in einem Mitgliedstaat der Europäischen Union statt. Jede Offenlegung von vertragsgegenständlichen personenbezogenen Da-

ten gegenüber einem Empfänger in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und der Beachtung der Voraussetzungen der Art. 44 ff. DS-GVO.

1.5. Angabe der Datenarten und deren Schutzbedarf:

☐ Interne Daten
(normaler Schutzbedarf, Schutzklasse 1)

☐ Nicht allgemein zugängliche personenbezogene und vertrauliche Daten
(hoher Schutzbedarf, Schutzklasse 2)

☐ Geheime Daten
(sehr hoher Schutzbedarf, Schutzklasse 3)

1.6. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Kunden	☐ Geschäftspartner
☐ Beschäftigte	☐ Interessenten
☐ Lieferanten	☐ Abonnenten
☐ Berater/Handelsvertreter	☐
☐ Ansprechpartner	☐

2. Weisungsbefugnisse des Auftraggebers

2.1. Der Auftragnehmer verpflichtet sich, die Auftragsverarbeitung grundsätzlich nur nach den vertraglichen Vorgaben durchzuführen, die der Auftraggeber im Einzelfall durch Weisungen konkretisieren kann. Dem Weisungsrecht unterliegt die Entscheidung, ob eine Verarbeitung stattfindet und welche Daten durch den Auftragnehmer verarbeitet werden. Die Entscheidung über die Mittel der Verarbeitung trifft allein der Auftraggeber, indes besteht eine vertragliche Pflicht zur Ausführung der Verarbei-

tung mit bestimmten Mitteln oder auf bestimmte Art und Weise nur nach vorheriger Einigung der Parteien, die auch die entsprechende Gegenleistung des Auftraggebers umfasst. Das Weisungsrecht erstreckt sich nicht auf die von Auftragnehmer zu ergreifenden technischen und organisatorischen Maßnahmen und findet im Allgemeinen seine Grenzen in dieser Vereinbarung.

2.2. Weisungen für die Auftragsverarbeitung hat der Auftraggeber dem Auftragnehmer mind. in Textform mitzuteilen.

2.3. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltendes Datenschutzrecht (Beanstandung). Der Auftragnehmer ist berechtigt, die Durchführung der beanstandeten Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt wird. Auch eine Bestätigung ist nur wirksam, wenn sie mindestens in Textform mitgeteilt wird.

2.4. Der Auftragnehmer ist zu Verarbeitungen jenseits der vertraglichen Vorgaben berechtigt, sofern der Auftragnehmer durch das Recht der Europäischen Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Ausführung einer solchen Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3. Zur Verarbeitung eingesetzte Personen

Der Auftragnehmer verpflichtet sich, zur Durchführung der Verarbeitungen nur Personen einzusetzen, die er auf die Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Ferner verpflichtet er sich, diese Personen zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen.

4. Technische und organisatorische Maßnahmen

4.1. Der Auftragnehmer schuldet im Hinblick auf die vertragsgegenständlichen Art(en) von Verarbeitungen – neben seiner eigenen Verpflichtung aus Art. 32 Abs. 1 DS-GVO – kraft dieser Vereinbarung auch die Umsetzung der dem Auftraggeber insoweit gem. Art. 32 Abs. 1 DS-GVO obliegenden Maßnahmen, soweit diese nachfolgend festgelegt sind. Er sichert die Umsetzung dieser technischen und organisatorischen Maßnahmen zu, die hiermit festgelegt werden auf die Maßnahmen, die sich im Einzelnen ergeben aus der bei Vertragsschluss gültigen Norm DIN 66399-3, Tabelle 1, 3, 4 und 5.

4.2. Dem Auftragnehmer ist es gestattet, einseitig Änderungen an den Festlegungen zu technischen und organisatorischen Maßnahmen vorzunehmen. Eine solche Änderung der Festlegungen zu technischen und organisatorischen Maßnahmen durch den Auftragnehmer ist jedoch nur zulässig, wenn dadurch das Schutzniveau der vorhandenen Maßnahmen unmittelbar vor der geplanten Änderung in seiner Summe durch die Änderungen nicht abgesenkt wird. Änderungen der Festlegungen dürfen insbesondere vorgenommen werden wegen Änderungen der gesetzlichen Rahmenbedingungen sowie gerichtlicher oder behördlicher Vorgaben gegenüber dem Auftraggeber, dem Auftragnehmer oder einem anderen Kunden des Auftragnehmers, der dieselbe standardisierte Leistung des Auftragnehmers in Anspruch nimmt, die eine Änderung notwendig machen. Unter Beachtung der Vorgaben für das Schutzniveau können durch Änderungen zuvor festgelegte einzelne Maßnahmen gänzlich entfallen, ohne dass sie durch artverwandte Maßnahmen ersetzt werden müssen.

4.3. Änderungen sind durch den Auftragnehmer zu dokumentieren. Dem Auftraggeber sind jederzeit auf dessen Verlangen die vollständigen und aktuellen Festlegungen zu technischen und orga-

nisatorischen Maßnahmen im Hinblick auf die vertragsgegenständlichen Verarbeitungen vorzulegen.

5. Unterauftragsverhältnisse

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger schriftlicher Zustimmung des Auftraggebers beauftragen.

☐ Eine Unterbeauftragung ist unzulässig.

☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DS-GVO:

Unterauftragnehmer	Anschrift/Land	Leistung

6. Rechte betroffener Personen

6.1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich zwecks Geltendmachung ihrer Rechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten, sofern für den Auftragnehmer unschwer erkennbar ist, dass sich die betroffene Person an den Auftraggeber wenden möchte. Diese Vereinbarung steht der Erfüllung der Pflichten des Auftragnehmers aus

Art. 15 Abs. 1, 1. Halbsatz DS-GVO nicht entgegen, soweit sich betroffene Personen an ihn als Verantwortlichen wenden.

6.2. Angesichts der vertragsgegenständlichen Art(en) der Verarbeitung bietet der Auftragnehmer dem Auftraggeber an, ihn mit technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 12 bis 23 DS-GVO genannten Rechte der betroffenen Person nachzukommen. Die Parteien werden sich über die Geeignetheit konkreter Maßnahmen austauschen und über die kaufmännischen Bedingungen der Realisierung dieser Maßnahmen gesondert einigen.

7. Mitteilung bei Verletzungen des Schutzes personenbezogener Daten und Unterstützungsleistungen des Auftragnehmers

7.1. Dem Auftragnehmer ist seine Meldepflicht gegenüber dem Auftraggeber aus Art. 33 Abs. 2 DS-GVO bekannt, die anders als die Meldepflicht des Auftraggebers gegenüber der Aufsichtsbehörde nicht durch eine Risikoprognose eingeschränkt ist. Meldungen wird der Auftragnehmer an folgende Adresse bzw. Kontaktperson richten:

_____

7.2. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der vertragsgegenständlichen Art(en) der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der dem Auftraggeber aus den Artikeln 32 bis 36 DS-GVO erwachsenden Pflichten. Unterstützungsleistungen erbringt der Auftragnehmer im Zweifel auf Abruf und nur soweit ihm das Verlangen der Unterstützungsleistung zumutbar ist.

7.3. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

8. Löschung und Rückgabe von personenbezogenen Daten

Die überlassenen Akten und Datenträger werden vernichtet. Im normalen Geschäftsgang sind nach Abschluss der Erbringung der Verarbeitungsleistungen keine personenbezogenen Daten mehr beim Auftragnehmer vorhanden, die ihm zuvor vom Auftraggeber unter dieser Vereinbarung überlassen wurden und die nach Wahl des Auftraggebers entweder gelöscht oder zurückgegeben werden könnten. Sollten aufgrund von Unregelmäßigkeiten Daten noch vorhanden sein, ist der Auftraggeber unverzüglich zu benachrichtigen; ihm steht dann vorgenanntes Wahlrecht zu.

9. Kontrollrechte des Auftraggebers

9.1. Der Auftraggeber hat das Recht, beim Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftraggeber kann von vor Ort Kontrollen absehen und stattdessen die Zusendung von durch ihn zu bestimmenden Auskünften in schriftlicher Form binnen angemessener Frist vom Auftragnehmer verlangen.

9.2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO und dieser Vereinbarung überzeugen kann. Der Auftrag-

nehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen i.S.v. Ziff. 4 nachzuweisen.

9.3. Der Nachweis solcher technischer und organisatorischer Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ *die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO*
- ☐ die *Zertifizierung nach DIN 66399 bzw. ISO 21964*
- ☐ *Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)*

9.4. Für die Ermöglichung von bzw. Mitwirkung an Kontrollen vor Ort kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

10. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

10.1. Der Auftragnehmer hat ergänzend zu den Pflichten aus dieser Vereinbarung gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO, die ihm bekannt sind und deren Erfüllung – nebst Nachweisen für diese – er dem Auftraggeber hiermit zusichert.

10.2. Zusätzlich gewährleistet er die Einhaltung folgender Vorgaben:

a) Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausüben kann – unabhängig davon, ob der Auftragnehmer kraft Gesetzes einen Datenschutzbeauftragten benennen muss. Dessen jeweils aktu-

elle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich zu hinterlegen.

b) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen einer Behörde, auch soweit sie sich nicht auf diesen Auftrag beziehen. Dies gilt insbesondere, soweit eine Behörde wegen des Verdachts einer Ordnungswidrigkeit oder einer Straftat in Bezug auf eine Verarbeitung personenbezogener Daten beim Auftragnehmer ermittelt.

c) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

d) Nachweisbarkeit der vertragsgegenständlichen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziff. 9 dieser Vereinbarung.

---	---
Ort, Datum	Ort, Datum
---	---
Auftraggeber	Auftragnehmer

8.2 Aufbewahrungsfristen (Stand: März 2019)

Checkliste: Wichtige gesetzliche Aufbewahrungspflichten/-fristen

Personenbezogene Daten sind zu löschen, sofern Art. 17 DS-GVO dies verlangt und keine Ausnahme davon greift, die ein Mitgliedstaat aufgrund einer Öffnungsklausel gesetzlich festgelegt hat. Die nachfolgende Checkliste erhebt keinen Anspruch auf Vollständigkeit. Es soll lediglich ein Überblick über wichtige gesetzliche Aufbewahrungsvorschriften in Deutschland gegeben werden, die einer Vernichtung von Unterlagen entgegenstehen können. Insoweit sind neben den Regelungen des Handels- und Steuerrechts (allgemeine Aufbewahrungspflichten) vor allem die Aufbewahrungsnormen und -fristen im Personalbereich zu beachten.

Die Abschnitte 1. und 2. sind in Anlehnung einer Checkliste der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), die Abschnitte 3. und 4. einem Leitfaden der Deutschen Krankenhausgesellschaft vom November 2006 entnommen.

1. Allgemeine Aufbewahrungspflichten

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage
Arbeitsanweisungen[1] und sonstige Organisationsunterlagen (zu Handelsbüchern, Inventaren etc.)	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 Handelsgesetzbuch (HGB) § 147 Abs. 1 Nr. 1, Abs. 3 Abgabenordnung (AO) § 6 Krankenhaus-Buchführungsverordnung (KHBV)
Buchungsbelege[2] bzw. Dokumentation von Verfahren mit Belegfunktion davon: Rechnungen	10 Jahre	§ 257 Abs. 1 Nr. 4, Abs. 4 HGB § 147 Abs. 1 Nr. 4, Abs. 3 AO § 6 (KHBV) § 14b Umsatzsteuergesetz (UStG)
Handels- oder Geschäftsbriefe[3] – empfangene Schreiben	6 Jahre[4]	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB § 147 Abs. 1 Nr. 2, Abs. 3 AO § 6 (KHBV)
Handels- oder Geschäftsbriefe – Wiedergabe der abgesendeten Schreiben	6 Jahre[5]	§ 257 Abs. 1 Nr. 3, Abs. 4 HGB § 147 Abs. 1 Nr. 3, Abs. 3 AO § 6 (KHBV)
(Handels-)Bücher bzw. Aufzeichnungen	10 Jahre	(§ 257 Abs. 1 Nr. 1, Abs. 4 HGB) § 147 Abs. 1 Nr. 1, Abs. 3 AO

[1] Dazu zählen auch Anweisungen zu Zugriffsberechtigungen.

[2] Buchungsbelege sollen nachweisen, dass einer Buchung auch ein tatsächlicher Sachverhalt zu Grunde liegt. Buchungspflichtig sind alle Vorgänge, die Einfluss auf die Vermögens-, Finanz- oder Ertragslage haben. Buchungsbelege sind z.B. Ein- und Ausgangsrechnungen, Quittungen.

[3] Als Geschäftsbrief (Handelsbrief) gilt jegliche Korrespondenz, die der Vorbereitung, der Durchführung oder der Rückgängigmachung eines Geschäftes dient.

[4] Soweit es sich zugleich um einen Buchungsbeleg handelt, gilt die höhere Frist von zehn Jahren.

[5] Vgl. vorhergehende Fußnote.

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage
Inventare (einschließlich Forderungsverzeichnisse)	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB § 147 Abs. 1 Nr. 1, Abs. 3 AO § 6 (KHBV)
Jahresabschlüsse (einschließlich dazugehöriger Berichte) und Lageberichte	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB § 147 Abs. 1 Nr. 1, Abs. 3 AO § 6 (KHBV)
Sonstige steuerrelevante Unterlagen	6 Jahre	§ 147 Abs. 1 Nr. 5, Abs. 3 AO

2. Besondere Aufbewahrungsfristen im Personalbereich

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage
Arbeitnehmerüberlassung – Geschäftsunterlagen des Verleihers	3 Jahre	§ 7 Abs. 2 Arbeitnehmerüberlassungsgesetz (AÜG)
Arbeitsmittelprüfung – Aufzeichnungen über Prüfungsergebnisse	mindestens bis zur nächsten Prüfung	§ 14 Abs. 7 Satz 1 Betriebssicherheitsverordnung (BetrSichV)
Arbeitszeitnachweise (allgemein)	2 Jahre	§ 16 Abs. 2 Arbeitszeitgesetz (ArbZG)
DEÜV-Bescheinigung über Datenübermittlungen	bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres[6]	§ 25 Datenerfassungs- und -übermittlungsverordnung (DEÜV)
Fahrtenschreiber-Schaublätter	1 Jahr	§ 57a Abs. 2 Straßenverkehrszulassungsordnung (StvZO)
Fahrtkostenerstattung	6 Jahre	§ 41 Abs. 1 EStG i.V.m. R 9.5 der Lohnsteuerrichtlinien
Heimarbeit-Entgeltbelege	3 Jahre	§ 13 Erste Verordnung zur Durchführung des Heimarbeitsgesetzes (HAGDV 1)

Art der Unterlage	Aufbewahrungs-dauer	Rechtsgrundlage
Heimarbeit-Personenlisten	bis zum Ablauf des Kalenderjahres, das auf das Jahr der Anlegung folgt	§ 9 Abs. 3 (HAGDV 1)
Infektionsschutzgesetz-Gesundheitszeugnis und letzte Dokumentation der Belehrung	bis zum Ausscheiden des Arbeitnehmers	§ 43 Abs. 5 Infektionsschutzgesetz (IfSG)
Jugendarbeitsschutz-Unterlagen	2 Jahre	§ 50 Abs. 2 Jugendarbeitsschutzgesetz (JArbSchG)
Ladenschlussgesetz-Verzeichnisse und Unterlagen	1 Jahr	§ 22 Abs. 3 Nr. 2 Gesetz über den Ladenschluss (LadSchlG)
Lohnkonto (Steuer)	6 Jahre	§ 41 Abs. 1 EStG

[6] Prüfungen erfolgen mindestens alle 4 Jahre (§ 28p Abs. 1 Satz 1 Sozialgesetzbuch - Viertes Buch).

Art der Unterlage	Aufbewahrungs-dauer	Rechtsgrundlage
Lohnsteuerkarte	aktuelle Lohnsteuerkarte; Aushändigung nach Ablauf des Kalenderjahres oder bei Beendigung des Dienstverhältnisses vor Ablauf des Kalenderjahres [7]	§§ 39b Abs. 1, 41b Abs. 1 Satz 4 bis 6 EStG
Lohnsteuerpauschalierung	6 Jahre	§ 4 Abs. 2 Nr. 8 Lohnsteuer-Durchführungsverordnung (LStDV) i.V.m. § 41 Abs. 1 EStG
Lohnunterlagen[8] (Sozialversicherung)	bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres[9]	§ 28f Abs. 1 Satz 1 Sozialgesetzbuch - Viertes Buch (SGB IV)
Mutterschutz — Unterlagen	bis zum Ablauf von zwei Jahren nach der letzten Eintragung	§ 27 Abs. 5 Mutterschutzgesetz (MuSchG)

[7] § 41b Abs. 1 Satz 4 bis 6 Einkommensteuergesetz: „Nach Ablauf des Kalenderjahres darf der Arbeitgeber die Lohnsteuerkarte nur aushändigen, wenn sie eine Lohnsteuerbescheinigung enthält und der Arbeitnehmer zur Einkommensteuer veranlagt wird. Dem Arbeitnehmer nicht ausgehändigte Lohnsteuerkarten ohne Lohnsteuerbescheinigungen kann der Arbeitgeber vernichten; nicht ausgehändigte Lohnsteuerkarten mit Lohnsteuerbescheinigungen hat er dem Betriebsstättenfinanzamt einzureichen." „So-

weit der Arbeitgeber nicht zur elektronischen Übermittlung nach Absatz 1 Satz 2 verpflichtet ist, hat er nach Ablauf des Kalenderjahres oder wenn das Dienstverhältnis vor Ablauf des Kalenderjahres beendet wird, eine Lohnsteuerbescheinigung nach amtlich vorgeschriebenem Muster auszustellen. Er hat dem Arbeitnehmer diese Bescheinigung auszuhändigen. Nicht ausgehändigte Lohnsteuerbescheinigungen hat der Arbeitgeber dem Betriebsstättenfinanzamt einzureichen.

[8] Der notwendige Inhalt der Lohnunterlagen ist in § 2 der Verordnung über die Durchführung der Beitragsüberwachung und die Auskunfts- und Vorlagepflichten geregelt.

[9] Prüfungen erfolgen mindestens alle 4 Jahre (§ 28p Abs. 1 Satz 1 Sozialgesetzbuch - Viertes Buch).

3. Arbeitsschutzunterlagen

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage
Unterweisungsaufzeichnungen für bestimmte Beschäftigte im Sperrbereich und außerhalb des Kontrollbereichs	5 Jahre	§ 38 Abs. 4 Strahlenschutzverordnung (StrlSchV)
Unterweisungsaufzeichnungen für andere Personen im Kontrollbereich	1 Jahr	§ 38 Abs. 4 StrlSchV
Protokoll der Funktionsprüfung und Wartung von Strahlungsmessgeräten	10 Jahre	§ 67 Abs. 2 StrlSchV
Kartei über arbeitsmedizinische Vorsorgeuntersuchungen	Bis Ausscheiden des Mitarbeiters (außer Rechtsvorschriften oder die nach § 9 Abs. 4 bekannt gegebenen Regeln bestimmen etwas anderes) sowie Aushändigung eines Auszugs an die betroffene Person	§ 3 Abs. 4 ArbMedVV
Messprotokoll der Ortsdosis/-leistung im betrieblichen Überwachungsbereich einer Röntgeneinrichtung oder eines Störstrahlers	30 Jahre	§ 34 Röntgenverordnung (RöV)
Unterweisungsaufzeichnungen für bestimmte Beschäftigte im Sperrbereich und außerhalb des Kontrollbereichs	5 Jahre	§ 36 Abs. 4 RöV, § 38 Abs. 4 Strahlenschutzverordnung (StrlSchV)

Art der Unterlage	Aufbewahrungs-dauer	Rechtsgrundlage
Unterweisungsaufzeichnungen für andere Personen im Kontrollbereich	1 Jahr	§ 36 Abs. 4 RöV, § 38 Abs. 4 StrlSchV
Protokoll der Funktionsprüfung und Wartung von Strahlungsmessgeräten	10 Jahre	§ 67 Abs. 2 StrlSchV
Kartei über Vorsorgeuntersuchungen und ärztliche Bescheinigungen	Bis zum Ausscheiden des Mitarbeiters	z.B. § 11 Abs. 4 Unfallverhütungsvorschrift (UVV), BGV A4 Arbeitsmedizinische Vorsorge

Art der Unterlage	Aufbewahrungs-dauer	Rechtsgrundlage
Chemikalien (Prüfpläne, vorgenommene Inspektionen, Einweisungen, u.a.m.)	15 Jahre	Anhang 1 zu § 19a Abs. 1 Chemikaliengesetz (ChemG)
Gefährliche Arbeitsstoffe	30 Jahre[10]	früher: § 18 Gefahrstoffverordnung (GefStoffV)
Eintragung oder Einstellung eines Vorgangs über die Entsorgung gefährlicher Abfälle in ein Register	3 Jahre	§ 49 Abs. 1 und 3 i.V.m. Abs. 5 KrWG
Eintragung oder Einstellung eines Vorgangs über die Beförderung gefährlicher Abfälle in ein Register	mindestens 1 Jahr	§ 49 Abs. 1 und 3 i.V.m. Abs. 5 KrWG

[10] Empfehlung aus Beweissicherungsgründen, da Aufbewahrungsfrist bei Novellierung 2005 abgeschafft wurde.

4. Medizinische Unterlagen

Art der Unterlage	Aufbewahrungs-dauer	Rechtsgrundlage
Behandlungsunterlagen (Anamnese, Aufnahme- und Aufklärungsbögen, Befunde, Medikation, Pflegeanordnungen, Arztbriefe, EKG, EEG, CTG, histologische Berichte, OP-Berichte u.s.w.)	30 Jahre[11]	Nach § 10 Abs. 3 MBO (Stand 2019) 10 Jahre nach Abschluss der Behandlung; Verjährungsfristen lt. BGB: 30 Jahre
Aufzeichnungen, Röntgenbilder, digitale Bilddateien und sonstige Untersuchungsunterlagen im Fall	Bis zur Vollendung ihres 28. Lebensjahres	§ 85 Abs. 2 Nr. 2 b) Strahlenschutzgesetz (StrlSchG)

Art der Unterlage	Aufbewahrungs-dauer	Rechtsgrundlage
der **Untersuchung einer minderjährigen Person** bei Anwendung ionisierender Stoffe oder radioaktiver Strahlung		
Aufzeichnungen, Röntgenbilder, digitale Bilddateien und sonstige Untersuchungsunterlagen im Fall der **Untersuchung einer volljährigen Person** bei Anwendung ionisierender Stoffe oder radioaktiver Strahlung	10 Jahre	§ 85 Abs. 2 Nr. 2 a) StrlSchG
Aufzeichnungen, Röntgenbilder, digitale Bilddateien und sonstige Untersuchungsunterlagen im Fall der **Behandlung einer Person** bei Anwendung ionisierender Stoffe oder radioaktiver Strahlung	30 Jahre	§ 85 Abs. 2 Nr. 1 StrlSchG
Aufzeichnungen zur Konstanzprüfung i.S.d. § 116 StrlSchV	10 Jahre	§ 117 StrlSchV
Einwilligungen und Aufzeichnungen im Zusammenhang mit der Anwendung von radioaktiven Stoffen oder ionisierender Strahlung zum Zweck der medizinischen Forschung, Aufzeichnungen im Rahmen der klinischen Forschung im Zusammenhang mit Röntgen und Bestrahlung	30 Jahre	§ 140 StrlSchV

[11] Empfehlung aus Beweissicherungsgründen.

Art der Unterlage	Aufbewahrungs-dauer	Rechtsgrundlage
Aufzeichnungen zur Qualitätssicherung vor Inbetriebnahme; Abnahmeprüfung i.S.d. § 115 StrlSchV	Für die Dauer des Betriebes, mindestens 3 Jahre nach Abschluss der letzten Prüfung	§ 117 StrlSchV
Unterlagen über Verbleib und Bestand von Betäubungsmitteln	3 Jahre von der letzten Eintragung gerechnet	§ 13 Abs. 3 Betäubungsmittelverschreibungsverordnung (BtMVV)

Art der Unterlage	Aufbewahrungs-dauer	Rechtsgrundlage
Aufzeichnungen über Herstellung, Prüfung, Lagerung, Einfuhr, Rückruf usw. von Arzneimitteln	mindestens 1 Jahr nach Ablauf des Verfallsdatums, jedoch nicht weniger als 5 Jahre	§ 22 Abs. 1 Apothekenbetriebsordnung (ApBetrO)
Aufzeichnungen über Rückverfolgung zum Unterzeichner bei Verschreibung in elektronischer Form	3 Jahre nach der letzten Eintragung	§ 22 Abs. 1b ApBetrO
Aufzeichnungen zur Rückverfolgung hinsichtlich Erwerbs und Abgabe von Blutzubereitungen, Sera Plasmaproteinen usw.	mindestens 30 Jahre	§ 22 Abs. 4 ApBetrO
Aufzeichnungen über Blutspendenentnahme	mindestens 15 Jahre	§ 11 Abs. 1 Transfusionsgesetz (TFG)
Immunisierungsprotokolle und Aufzeichnungen im Zusammenhang mit der Vorbehandlung zur Blutstammzellseparation	mindestens 20 Jahre	§ 11 Abs. 1 TFG
Angaben zur Spenderdokumentation, die für die Rückverfolgung benötigt wird	mindestens 30 Jahre	§ 11 Abs. 1 TFG
Aufzeichnungen über Blutdepots, die Blutprodukte lagern und abgeben	mindestens 30 Jahre	§ 11a TFG i.V.m. § 15 Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHW)
Aufzeichnungen über die Anwendung von Blutprodukten	mindestens 30 Jahre	§ 14 Abs. 3 TFG
Aufzeichnungen im Zusammenhang mit der Anwendung von Blutprodukten (Aufklärung, Einwilligungserklärungen usw.)	mindestens 15 Jahre	§ 14 Abs. 3 TFG
Transplantationsunterlagen	mindestens 10 Jahre	§ 15 TPG
Berufsgenossenschaftliche Verletzungsverfahren	mindestens 15 Jahre	Anforderungen nach § 34 SGB VII

8.3 Vereinbarung zur Geheimhaltung

Vereinbarung

zwischen

- Berufsgeheimnisträger - nachstehend Auftraggeber genannt

und

- mitwirkende Person - nachstehend Auftragnehmer genannt

Der Auftraggeber hat den Auftragnehmer mit der Erbringung von Leistungen der Akten- und Datenträgervernichtung beauftragt. In diesem Zusammenhang wird der Auftraggeber dem Auftragnehmer, soweit dies zur Inanspruchnahme der Leistungen des Auftragnehmers erforderlich ist, den Zugang zu Informationen eröffnen, auf die sich die Verpflichtung des Auftraggebers zur Geheimhaltung nach § 203 StGB bezieht.

Ausschließlich zum Zwecke der Vermeidung einer Strafbarkeit des Auftraggebers bzw. der für ihn handelnden Personen gem. § 203 Abs. 4 Satz 2 Nr. 1 StGB wird der Auftragnehmer hiermit im Sinne dieser Norm zur Geheimhaltung verpflichtet.

Dem Auftragnehmer ist bekannt, dass er kraft Gesetzes – ungeachtet dieser Vereinbarung – zur Geheimhaltung aller Informationen verpflichtet ist, die dem Auftraggeber bei Ausübung seiner die Geheimhaltungspflicht begründenden Tätigkeit bekannt geworden sind und zu denen der Auftraggeber ihm den Zugang eröffnet hat. Die Vorschriften über den Schutz personenbezogener Daten bleiben von dieser Vereinbarung unberührt.

---	---
Ort, Datum	Ort, Datum
---	---
Auftraggeber	Auftragnehmer

Satzung

der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. (in der Fassung der Beschlüsse vom 10.11.1983, 16.11.1984, 14.11.1990, 04.11.1991, 20.11.2002, 18.11.2009 und 21.11.2012 der ordentlichen Mitgliederversammlung in Köln)

Präambel

Datenschutz und Datensicherheit sind mit Blick auf die modernen Informations- und Kommunikationstechnologien sowie den wachsenden wirtschaftlichen Wert personenbezogener Daten wichtige Grundpfeiler der Informationsgesellschaft. Ein angemessener Datenschutz hat dabei sowohl dem Recht auf informationelle Selbstbestimmung als auch der Informationsfreiheit Rechung zu tragen. Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. tritt für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen und deren Datenschutzbeauftragte bei der Lösung der vielfältigen technischen, rechtlichen und organisatorischen Fragen zu unterstützen, die durch das Erfordernis nach rechtmäßiger, ordnungsgemäßer und sicherer Datenverarbeitung aufgeworfen werden. Die Gesellschaft tritt hierzu für die Prinzipien der Selbstkontrolle und Selbstregulierung ein. Im Rahmen ihrer Aktivitäten pflegt sie eine intensive Zusammenarbeit mit Wirtschaft, Verwaltung, Wissenschaft und Politik. Die Gesellschaft vertritt die Belange der Daten verarbeitenden Stellen - insbesondere auch der mittelständischen Wirtschaft -, deren Datenschutzbeauftragten und der betroffenen Bürger gegenüber Regierungen und Gesetzgebungsorganen; sie will ferner die politische Willensbildung durch fachlichen Rat unterstützen.

§ 1
Name, Sitz, Geschäftsjahr

(1) Der Verein führt den Namen „Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.“ Die Gesellschaft hat ihren Sitz in Bonn; sie ist in das Vereinsregister eingetragen.

(2) Das Geschäftsjahr der Gesellschaft ist das Kalenderjahr.

§ 2
Zweck und Gemeinnützigkeit

(1) Die Gesellschaft mit Sitz in Bonn verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne des Abschnitts „Steuerbegünstigte Zwecke“ der Abgabenordnung. Zweck der Gesellschaft ist die Förderung der Volks- und Berufsbildung auf dem Gebiet des Datenschutzes und der Datensicherheit im Sinne der dieser Satzung vorangestellten Präambel. Der Satzungszweck wird verwirklicht insbesondere durch

1. die Zurverfügungstellung von Informationen und Materialien an die betroffenen Bürger und Daten verarbeitenden Stellen zur Meinungsbildung und Entscheidungsfindung,
2. die Bildung von Arbeits- und Erfahrungsaustauschkreisen,
3. die Entwicklung und Veröffentlichung von Methoden zur Sicherung der Qualifikation von Datenschutzverantwortlichen, insbesondere Datenschutzbeauftragten,
4. die Zusammenarbeit mit den in der Datenschutzgesetzgebung vorgesehenen staatlichen Kontrollorganen.

(2) Die Gesellschaft ist selbstlos tätig; sie verfolgt nicht in erster Linie eigenwirtschaftliche Zwecke. Mittel der Gesellschaft dürfen nur für die satzungsmäßigen Zwecke verwendet werden. Die Mitglieder erhalten keine Zuwendungen aus Mitteln der Gesellschaft. Es darf keine Person durch Ausgaben, die dem Zweck der Gesellschaft fremd sind, oder durch unverhältnismäßig hohe Vergütungen begünstigt werden.

§ 3
Mitgliedschaft

(1) Ordentliche Mitglieder der Gesellschaft können natürliche und juristische Personen, Handelsgesellschaften, nicht rechtsfähige Ver-

eine sowie Anstalten und Körperschaften des öffentlichen Rechts werden.
(2) Die Beitrittserklärung erfolgt schriftlich gegenüber dem Vorstand. Über die Annahme der Beitrittserklärung entscheidet der Vorstand. Die Mitgliedschaft beginnt mit Annahme der Beitrittserklärung.
(3) Die Mitgliedschaft endet durch Austrittserklärung, durch Tod von natürlichen Personen oder durch Auflösung und Erlöschen von juristischen Personen, Handelsgesellschaften, nicht rechtsfähigen Vereinen sowie Anstalten und Körperschaften des öffentlichen Rechts oder durch Ausschluss; die Beitragspflicht für das laufende Geschäftsjahr bleibt hiervon unberührt.
(4) Der Austritt ist nur zum Schluss eines Geschäftsjahres zulässig; die Austrittserklärung muss spätestens drei Monate vor Ablauf des Geschäftsjahres gegenüber dem Vorstand schriftlich abgegeben werden.
(5) Die Mitgliederversammlung kann solche Personen, die sich besondere Verdienste um die Gesellschaft oder um die von ihr verfolgten satzungsgemäßen Zwecke erworben haben, zu Ehrenmitgliedern ernennen. Ehrenmitglieder haben alle Rechte eines ordentlichen Mitglieds. Sie sind von Beitragsleistungen befreit.

§ 4
Rechte und Pflichten der Mitglieder

(1) Die Mitglieder sind berechtigt, die Leistungen der Gesellschaft in Anspruch zu nehmen.
(2) Die Mitglieder sind verpflichtet, die satzungsgemäßen Zwecke der Gesellschaft zu unterstützen und zu fördern. Sie sind ferner verpflichtet, die festgesetzten Beiträge zu zahlen.

§ 5
Ausschluss eines Mitgliedes

(1) Ein Mitglied kann durch Beschluss des Vorstandes ausgeschlossen werden, wenn es das Ansehen der Gesellschaft schädigt, seinen Beitragsverpflichtungen nicht nachkommt oder wenn ein sonstiger wichtiger Grund vorliegt. Der Vorstand muss dem auszuschließenden Mitglied den Beschluss in schriftlicher Form unter der Angabe der Gründe mitteilen und ihm auf Verlangen eine Anhörung gewähren.
(2) Gegen den Beschluss des Vorstandes ist die Anrufung der Mitgliederversammlung zulässig. Bis zum Beschluss der Mitgliederversammlung ruht die Mitgliedschaft.

§ 6
Beitrag

(1) Die Gesellschaft erhebt einen Jahresbeitrag. Er ist für das Geschäftsjahr im ersten Quartal des Jahres im Voraus zu entrichten. Das Nähere regelt die Beitragsordnung, die von der Mitgliederversammlung beschlossen wird.
(2) Im begründeten Einzelfall kann für ein Mitglied durch Vorstandsbeschluss ein von der Beitragsordnung abweichender Beitrag festgesetzt werden.

§ 7
Organe der Gesellschaft

Die Organe der Gesellschaft sind
1. die Mitgliederversammlung,
2. der Vorstand.

§ 8
Mitgliederversammlung

(1) Oberstes Beschlussorgan ist die Mitgliederversammlung. Ihrer Beschlussfassung unterliegen
1. die Genehmigung des Finanzberichtes und der Haushaltspläne,
2. die Entlastung des Vorstandes,
3. die Wahl der einzelnen Vorstandsmitglieder,
4. die Bestellung von Finanzprüfern,
5. Satzungsänderungen,
6. die Genehmigung der Beitragsordnung,
7. die Richtlinie für die Erstattung von Reisekosten und Auslagen,
8. Anträge des Vorstandes und der Mitglieder,
9. die Ernennung von Ehrenmitgliedern,
10. die Auflösung der Gesellschaft.

(2) Die ordentliche Mitgliederversammlung findet einmal im Jahr statt. Außerordentliche Mitgliederversammlungen werden auf Beschluss des Vorstandes abgehalten, wenn die Interessen der Gesellschaft dies erfordern, oder wenn ein Viertel der Mitglieder dies unter Angabe des Zweckes schriftlich beantragt. Die Einberufung der Mitgliederversammlung erfolgt schriftlich durch den Vorstand mit einer Frist von mindestens zwei Wochen.

Hierbei sind die Tagesordnung bekannt zugeben und ihr die nötigen Informationen beizufügen, insbesondere Geschäftsbericht, Finanzbericht, Haushaltsplan, Satzungsänderungen, Änderungen der Beitragsordnung und - soweit bekannt - Wahlvorschläge und Anträge an die Mitgliederversammlung. Anträge zur Tagesordnung sind mindestens drei Tage vor der Mitgliederversammlung bei der Geschäftsstelle einzureichen. Über die Behandlung von Initiativanträgen entscheidet die Mitgliederversammlung.

(3) Die Mitgliederversammlung ist beschlussfähig, wenn mindestens 30 stimmberechtigte Mitglieder anwesend sind. Beschlüsse sind jedoch gültig, wenn die Beschlussfähigkeit vor der Beschlussfassung nicht angezweifelt worden ist.

(4) Beschlüsse über Satzungsänderungen und über die Auflösung der Gesellschaft bedürfen zu ihrer Rechtswirksamkeit der Dreiviertelmehrheit der anwesenden und ordnungsgemäß vertretenen Mitglieder. In allen anderen Fällen genügt die einfache Mehrheit.

(5) Jedes Mitglied hat eine Stimme. Juristische Personen haben einen Stimmberechtigten schriftlich zu bestellen. Jedes Mitglied hat das Recht, sich durch eine andere stimmberechtigte natürliche Person vertreten zu lassen; eine Person kann höchstens zehn Stimmen auf sich vereinigen. Die Bestellung des Vertreters hat schriftlich zu erfolgen.

(6) Auf Antrag des Mitglieds ist geheim abzustimmen. Über die Beschlüsse der Mitgliederversammlung ist ein Protokoll anzufertigen, das vom Versammlungsleiter und dem Protokollführer zu unterzeichnen ist; das Protokoll ist allen Mitgliedern zuzustellen und auf der nächsten Mitgliederversammlung genehmigen zu lassen.

§ 9
Vorstand

(1) Der Vorstand besteht aus mindestens sieben und höchstens elf Mitgliedern:

1. dem Vorsitzenden,
2. zwei stellvertretenden Vorsitzenden,
3. dem Schatzmeister,
4. mindestens zwei und maximal sechs Beisitzern und
5. dem Erfa-Repräsentanten.

Der Vorstand ist berechtigt, bei entsprechendem Bedarf bis zu zwei Mitglieder zu kooptieren. Diese haben kein Stimmrecht.

(2) Vorstand im Sinne des § 26 Abs. 2 BGB sind der Vorsitzende, im Verhinderungsfall sein Stellvertreter, zusammen mit einem der anderen Vorstandsmitglieder. Die Vertretungsmacht ist durch Beschlüsse des gesamten Vorstandes begrenzt.

(3) Der Vorstand beschließt mit der Mehrheit seiner satzungsgemäßen Mitglieder. Sind mehr als zwei Vorstandsmitglieder dauernd an der Ausübung ihres Amtes gehindert, so sind unverzüglich Nachwahlen anzuberaumen.

(4) Die Amtsdauer der Vorstandsmitglieder beträgt zwei Jahre; Wiederwahl ist zulässig.

(5) Der Vorstand gibt sich eine Geschäftsordnung.

(6) Der Vorstandsvorsitzende ist Dienstvorgesetzter der Geschäftsführer.

(7) Der Schatzmeister überwacht die Haushaltsführung und verwaltet das Vermögen der Gesellschaft. Er hat auf eine sparsame und wirtschaftliche Haushaltsführung hinzuwirken. Mit Ablauf des Geschäftsjahres stellt er unverzüglich die Abrechnung sowie die Vermögensübersicht und sonstige Unterlagen von wirtschaftlichem Belang den Finanzprüfern der Gesellschaft zur Prüfung zur Verfügung.

(8) Die Vorstandsmitglieder sind grundsätzlich ehrenamtlich tätig; sie haben Anspruch auf Erstattung notwendiger Auslagen im Rahmen einer von der Mitgliederversammlung zu beschließenden Richtlinie über die Erstattung von Reisekosten und Auslagen.

(9) Der Vorstand kann einen 'Wissenschaftlichen Beirat' einrichten, der für die Gesellschaft beratend und unterstützend tätig wird; in den Beirat können auch Nicht-Mitglieder berufen werden.

(10) Auf Vorschlag des Vorstandes kann die Mitgliederversammlung einen Vorsitzenden des Vorstandes nach dessen Ausscheiden aus dem Vorstand wegen herausragender Verdienste um die Gesellschaft zum Ehrenvorsitzenden ernennen. Der Ehrenvorsitzende wird zu den Sitzungen des Vorstandes eingeladen, er hat aber kein Stimmrecht.

§ 10
Geschäftsführung

(1) Die Geschäftsführung besteht aus bis zu zwei Geschäftsführern. Die Rechte und Pflichten werden in einem Dienstvertrag geregelt.

(2) Die Geschäftsführung führt die Geschäfte der Gesellschaft. Sie ist an die Vorgaben und Weisungen des Vorstandes gebunden. Die Geschäftsführung erstellt insbesondere den Jahreshaushaltsplan, den Rechnungsabschluss sowie den Geschäftsbericht und bereitet die Sitzungen des Vorstandes, der Mitgliederversammlung, des wissenschaftlichen Beirates und des Erfa-Beirates vor.

(3) Innerhalb des laufenden Geschäftsverkehrs ist die Geschäftsführung im Rahmen der ihr erteilten Vollmacht ermächtigt, den Verein zu verpflichten und Rechte für ihn zu erwerben.

§ 11
Finanzprüfer

(1) Zur Kontrolle der Haushaltsführung bestellt die Mitgliederversammlung Finanzprüfer. Nach Durchführung ihrer Prüfung geben sie dem Vorstand Kenntnis von ihrem Prüfungsergebnis und erstatten der Mitgliederversammlung Bericht.
(2) Die Finanzprüfer dürfen dem Vorstand nicht angehören.

§ 12
Erfa-Organisation

(1) Die Gesellschaft bildet zur Durchführung ihrer Aufgaben Erfahrungsaustauschkreise (Erfa-Kreise). Aufgabe der Erfa-Kreise ist es insbesondere, in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und sonstigen Fachleuten für Fragen des Datenschutzes und der Datensicherheit,

1. die Teilnehmer bei der Lösung und Klärung bestehender Datenschutzprobleme zu unterstützen,
2. auf lokaler oder regionaler Ebene Ziele und Belange der Gesellschaft und ihrer Mitglieder zu vertreten,
3. auf lokaler oder regionaler Ebene die Belange der betrieblichen Datenschutzbeauftragten zu vertreten.

(2) Aufgabe der Erfa-Kreise ist es ferner,

1. die Entscheidungsbildung in der Gesellschaft zu fördern und vorzubereiten,
2. Mitglieder für die Gesellschaft zu werben.

(3) Beabsichtigt ein Erfa-Kreis, bestimmte Themen oder Aktivitäten mit überregionalem Bezug an die Öffentlichkeit zu tragen, ist dies vorher mit dem Vorstand der Gesellschaft abzustimmen.
(4) Jeder Erfa-Kreis wählt einen Erfa-Kreis-Leiter. Die Erfa-Kreise sollten sich eine Geschäftsordnung geben, die mit dem Erfa-Beirat abzustimmen ist.

§ 13
Erfa-Beirat

(1) Der Erfa-Beirat besteht aus den Erfa-Kreis-Leitern, die Mitglieder der Gesellschaft sind.
(2) Der Erfa-Beirat schlägt der Mitgliederversammlung aus seiner Mitte den Erfa-Repräsentanten zur Wahl in den Vorstand vor.
(3) Der Erfa-Beirat wirkt bei der Führung der Geschäfte der Gesellschaft beratend und unterstützend mit. Er hat insbesondere die Aufgabe, die Belange der Erfa-Kreise zu vertreten.
(4) Der Erfa-Beirat gibt sich eine Geschäftsordnung; in ihr ist die Mitgliederstärke der einzelnen Erfa-Kreise angemessen zu berücksichtigen.

§ 14
Auflösung der Gesellschaft

Bei der Auflösung oder Aufhebung der Gesellschaft oder bei Wegfall steuerbegünstigter Zwecke fällt das Vermögen der Gesellschaft an eine juristische Person des öffentlichen Rechts oder eine andere steuerbegünstigte Körperschaft zwecks Verwendung für die Förderung der Volks- und Berufsbildung.

Nähere Informationen über die GDD finden Sie unter www.gdd.de oder rufen Sie uns an 0228/96 96 75 00.

Mitgliedschaft

GDD-Mitglieder können natürliche und juristische Personen, Personengesellschaften, nicht-rechtsfähige Vereine sowie Einrichtungen des öffentlichen Rechts im In- und Ausland werden. Bei Wirtschaftsunternehmen, Behörden, Verbänden u.ä. wird ein nach Größe der Vereinigung gestaffelter Jahresbeitrag erhoben. Einzelheiten ergeben sich aus unserer Beitragsordnung. Firmenmitglieder können neben den regelmäßigen Serviceleistungen der GDD zusätzlich die Unterstützung bei Datenschutzfragen aus der betrieblichen Praxis ihres Unternehmens in Anspruch nehmen. Wenn Sie Mitglied werden möchten, senden Sie bitte folgende Beitrittserklärung ausgefüllt an die

Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)
Heinrich-Böll-Ring 10 · 53119 Bonn · F +49 228 96 96 75 25 · info@gdd.de

.....

Beitrittserklärung

Für eine ordentliche Mitgliedschaft gem. § 3 Abs. 1 der GDD-Satzung:

☐ Firmenmitgliedschaft
Anzahl der Beschäftigten: .....
☐ Persönliche Mitgliedschaft (nur Privatpersonen)
☐ Persönliche Mitgliedschaft als betrieblicher Datenschutzbeauftragter

Firma: .....

Name: .....

Straße/Ort: .....

Abteilung/Branche: .....

Telefon-/Fax-Nr.: .....

E-Mail: .....

Ich möchte das GDD-Datenschutz-Jahrbuch zusätzlich zum eBook als PrintVersion erhalten

☐ ja ☐ nein

Mit der Aufnahme meiner Daten in die offizielle Mitgliederliste erkläre ich mich

☐ einverstanden ☐ nicht einverstanden

.....
Datum und Unterschrift

Wir verarbeiten Ihre Daten zu Ihrer Betreuung im Rahmen der Mitgliedschaft, ggf. auch unter Einsatz von Dienstleistern. Darüber hinaus geben wir Ihre Adressdaten an unseren Kooperationspartner Verlagsgruppe Hüthig Jehle Rehm GmbH – Datakontext – weiter, um Sie über Produkte und Fachveranstaltungen zum Thema Datenschutz und IT-Sicherheit zu informieren. Der Verwendung Ihrer Daten zu Werbezwecken können Sie jederzeit bei uns widersprechen.

>> GDD-Support für Wirtschaft, Verwaltung, Wissenschaft und Politik

Die GDD tritt für die Prinzipien der Selbstkontrolle und Selbstregulierung auf dem Gebiet des Datenschutzes ein. Sie unterstützt die politische Willensbildung durch fachlichen Rat.

Bei der Umsetzung der datenschutzrechtlichen Vorgaben bietet die GDD folgende Leistungen:

- >> Beratung in Einzelfragen
- >> Schulungen und Praktikerforen
- >> Online-Datenbanken, u.a.:
  GDD-Rechtsprechungsarchiv
  GDD-Literaturarchiv
- >> GDD-Praxis-Ratgeber
- >> Fachzeitschrift „Recht der Datenverarbeitung (RDV)"
- >> Fachpublikationen
- >> Erfahrungsaustausch

Wie Sie noch mehr erfahren

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

Heinrich-Böll-Ring 10
53119 Bonn
Telefon (0228) 96 96 75 00
Telefax (0228) 96 96 75 25
E-Mail: info@gdd.de
Internet: www.gdd.de

DIN 66399
ISO 21964

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.