Arbeitshilfe

„Ausgewählte Hinweise zur Umsetzung des Löschkonzepts“

Stand: April 2024

Inhaltsverzeichnis

Impressum:

Verband Thüringer Wohnungs- und Immobilienwirtschaft e.V. (vtw)
Regierungsstraße 58
99084 Erfurt
Telefon: 0361 / 360100
Internet: www.vtw.de
E-Mail: info@vtw.de

Ansprechpartnerin:
Uta Thiel
Referentin Digitalisierung/Neue Technologien

1. Vorwort

Die Datenschutz-Grundverordnung ist am 25. Mai 2018 in Kraft getreten. Wichtige Hinweise zur Umsetzung in der Wohnungswirtschaft erfolgten bereits durch die GdW Arbeitshilfe 83 und den vtw DSGVO-Leitfaden, welche in 2018 veröffentlicht wurden.

Seitdem haben die Wohnungsunternehmen umfangreiche Erfahrungen mit der Datenerfassung, -verarbeitung und -löschung insbesondere von personenbezogenen Daten (kurz pbD) gesammelt.

Eine Arbeitsgruppe des Fachausschusses „mediadigITal“ hat praxiserprobte Hinweise und Handlungsempfehlungen zusammengetragen, welche die vtw-Mitgliedsunternehmen in der Umsetzung des Löschkonzepts unterstützen sollen. Die Arbeitshilfe wird ergänzt durch mehrere Checklisten und ein Muster Löschprotokoll.

Mein Dank gilt insbesondere den Mitgliedern der Arbeitsgruppe „Umsetzung Löschkonzept“ des Fachausschusses „mediadigITal“:

Dr. Angela Wernicke
Weimarer Wohnstätte GmbH

David Golling
Allgemeine Wohnungsbaugenossenschaft "Eisenach" eG

Mario Kindel
Wohnungsbau-Genossenschaft Erfurt eG

Christian Koch
Wohnungsbaugenossenschaft Einheit eG, Erfurt

Uta Thiel
Verband Thüringer Wohnungs- und Immobilienwirtschaft e.V.

Inhaltliche Unterstützung erfolgte weiterhin durch:

Claudia Dithmar
Verband Thüringer Wohnungs- und Immobilienwirtschaft e.V.

Roger Palm
DOMUS Consult Wirtschaftsberatungsgesellschaft mbH

Frank Emrich
Verbandsdirektor

2. Datenschutzrechtlicher Hintergrund

1. Datenschutz-Grundverordnung DSGVO

Ziel der Datenschutz-Grundverordnung (DSGVO) ist insbesondere der „Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten und zum freien Verkehr solcher Daten“ (Art. 1 Abs. 1 DSGVO). Personenbezogene Daten sind gemäß Art. 4 Ziffer 1 DSGVO alle Informationen, „die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.“ In der Wohnungswirtschaft geht es im Kern um den Schutz der personenbezogenen Daten der Mietinteressenten, Mieter, Genossenschaftsmitglieder, Mitarbeitenden oder sonstiger Dritter.

2. Warum wird gelöscht?

Allen, die von der Verarbeitung pbD betroffen sind, wird ein Recht auf Löschung (sog. „Recht auf Vergessenwerden“) gemäß Art. 17 Abs. 1 DSGVO eingeräumt. Die Löschung muss (i.d.R.) auch ohne Geltendmachung des Anspruchs durch den Betroffenen von dem Verantwortlichen vorgenommen werden.

Das „Recht auf Vergessenwerden“ besteht, wenn:

- die Zweckbindung nicht mehr vorhanden ist
- die Einwilligung widerrufen wird, weil die Rechtsgrundlage fehlt
- ein Widerspruch eingelegt wird
- die Daten unrechtmäßig verarbeitet wurden
- ein Erfordernis vorliegt.

Ein Lösch- und Sperrkonzept definiert nach DSGVO die Dokumenten- und Datenkategorien, dokumentiert die Löschregeln und beschreibt die Vorgehensweise, wie personenbezogene Daten im Unternehmen verarbeitet und nach festgelegten Fristen gelöscht, anonymisiert oder pseudonymisiert werden müssen. Damit stellt es ein unterstützendes Hilfsmittel und eine orientierende Handlungsanleitung für das Unternehmen und für die Mitarbeitenden dar. Die Erstellung eines Löschkonzepts für das Unternehmen wird empfohlen.

In der Außenperspektive behandelt ein Löschkonzept vor allem personenbezogene Daten, die im Rahmen des Vermietungsprozesses und des Mietverhältnisses gespeichert und verarbeitet werden. Daneben werden in der Außenperspektive auch personenbezogene Daten abgebildet, die von Kreditoren, Debitoren und Gremienmitgliedern vorliegen.

In der Innenperspektive werden personenbezogene Daten von Mitarbeitenden und Bewerbern zugeordnet, die im Rahmen von Arbeits- und Ausbildungsverhältnissen gespeichert und verarbeitet werden.

3. Anforderungen der DSGVO an die Löschung pbD

1	**Art. 5**	**Grundsatz der Speicherbegrenzung** PbD müssen in einer Form gespeichert werden, welche die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dabei handelt es sich um festgelegte, eindeutige und legitime Zwecke. Die Daten sind auf das unbedingt erforderliche Mindestmaß zu beschränken. Wenn der Zweck endet, müssen die pbD gelöscht werden.
2	**Art. 17** **Art. 19**	**Recht auf Löschung („Recht auf Vergessenwerden“)** Die betroffene Person hat das Recht von dem Verantwortlichen zu verlangen, dass eigene pbD unverzüglich gelöscht werden, soweit keine der definierten Ausnahme gilt. Es besteht eine Mitteilungs-pflicht zur Information von Empfängern der Daten über die Löschung.
3	**Art. 13/14** **Art. 15**	**Transparenz und Informationspflicht** Neben dem Zweck der Datenverarbeitung ist der Betroffene vorab u.a. auch über die Speicherdauer bzw. die Kriterien zur Festlegung dieser Dauer zu informieren. Die Angaben zur Dauer sind auch bei einem Auskunftsersuchen des Betroffenen zu erteilen.
4	**Art. 12**	**Verfahrensvorgaben und Managementprozess** Die Löschung muss unverzüglich erfolgen. In Bezug auf ein Löschersuchen muss der Betroffene transparent über den Stand des Verfahrens bzw. die auf den Antrag ergriffenen Maßnahmen informiert werden. Die Frist hierzu beträgt i.d.R. einen Monat. Die Einhaltung der Vorgaben muss der Verantwortliche nachweisen können.
5	**Art. 24/25** **Art. 32**	**Technisch-organisatorische Maßnahmen** Der Verantwortliche muss technische und organisatorische Maßnahmen ergreifen, um für einen angemessenen Schutz der pbD im Sinne der DSGVO zu sorgen. Hierzu gehören auch datenschutz-freundliche Voreinstellungen (privacy-by-design/ privacy-by-default). Die Maßnahmen sind nach dem Stand der Technik zu validieren.
6	**Art. 5/24** **Art. 30**	**Nachweis- bzw. Rechenschaftspflicht** Der Verantwortliche ist für die rechtmäßige Verarbeitung sowie die wirksame Einhaltung der Grundsätze bei Verarbeitung von pbD nachweispflichtig (Rechenschaftspflicht). Die Fristen verschiedener Datenkategorien müssen auch im Verzeichnis der Verarbeitungs-tätigkeiten erfasst werden.

Tabelle 1: Anforderungen der DSGVO
Quelle: DOMUS Consult Präsentation „Löschen nach Konzept“ 2021

4. Begriffliche und rechtliche Abgrenzung

Die Möglichkeiten, wie mit pbD umgegangen werden kann, werden zunächst aus begrifflicher und rechtlicher Perspektive voneinander abgegrenzt.

Begriffliche Abgrenzung	
Löschung	wenn die **Verarbeitung und Nutzung** der pbD einer betroffenen Person **nicht mehr möglich** sind.
Vernichtung	wenn Daten **rückstandslos beseitigt** werden (Datenverarbeitungsmethode; Art. 4 Nr. 2 DSGVO). An dieser Stelle wird auf die DIN 66399 und die Inanspruchnahme externer Dienstleister verwiesen.
Anonymisierung	wenn pbD derart **verändert** werden, dass diese Daten nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer natürlichen Person zugeordnet werden können; als Löschung im Sinne der DSGVO anerkannt, wenn nicht ohne unverhältnismäßigen Aufwand Personenbezug wieder herstellbar ist (Aktenzeichen der Datenschutzbehörde DSB-D123.270/0009-DSB/2018 vom 05.12.2018).
Pseudonymisierung	wenn pbD durch ein **Pseudonym oder einen Code ersetzt** werden, um die Identifikation zu erschweren (Erwägungsgrund Art. 26 DSGVO). Pseudonymisieren stellt einen umkehrbaren Prozess dar.
Sperrung	wenn pbD gekennzeichnet werden, um ihre weitere Verarbeitung oder **Nutzung einzuschränken oder unzugänglich** aufzubewahren. Die Daten bleiben bestehen, der Zugriff auf die Daten ist unterbunden, so dass sie nicht mehr im Rahmen der ursprünglichen Zweckbestimmung verarbeitet werden (Art. 18 DSGVO, Erwägungsgrund Art. 67 DSGVO, § 35 BDSG).

Tabelle 2: Begriffliche Abgrenzung
Quelle: DOMUS Consult Präsentation „Löschen nach Konzept“ 2021

Rechtliche Abgrenzung	
Recht auf Löschung	Unkenntlichmachung elektronisch vorgehaltener pbD, wenn für die Speicherung keine Rechtsgrundlage bestand oder die Rechtsgrundlage nicht mehr besteht (Art. 17 Abs. 1 DSGVO).
Vernichtung	Unkenntlichmachung von pbD auf körperlichen Gegenständen, bspw. Entsorgung des Datenträgers.
Anonymisierung	Ist als Löschung pbD im Sinne der DSGVO anerkannt. Personenbezug ist nicht ohne unverhältnismäßigen Aufwand wiederherstellbar (Az. DSB-D123.270/0009-DSB-2018).
Pseudonymisierung	PbD, „die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.“ (Erwägungsgrund Art. 26 DSGVO)
Recht auf Einschränkung der Verarbeitung	Sperrung als Methode zur Einschränkung der Verarbeitung von pbD (Art. 18, Erwägungsgrund Art. 67 DSGVO, § 35 BDSG).

Tabelle 3: Rechtliche Abgrenzung
Quelle: DOMUS Consult Präsentation „Löschen nach Konzept“ 2021

5. Wann muss gelöscht werden?

Personenbezogene Daten durchlaufen einen Lebenszyklus, von der Erhebung bis zur Löschung, wobei Aufbewahrungs- und Löschfristen je nach Datenkategorie unterschiedlich lang sein können.

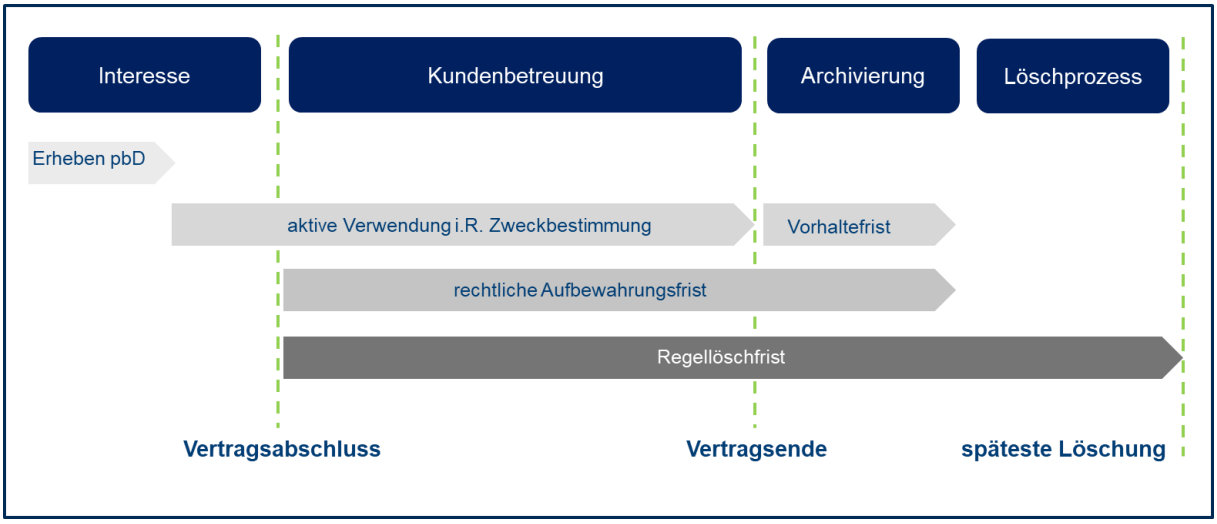

Abbildung 1: Lebenszyklus personenbezogener Daten
Quelle: DOMUS Consult Präsentation „Löschen nach Konzept“ 2021

6. Ausgewählte Aufbewahrungsfristen

Die Aufbewahrungsfristen beginnen immer erst **nach Ende des Kalenderjahres**, in dem im betreffenden Dokument die letzte Eintragung vorgenommen wurde.

Aufbewahrungsfristen	Datenkategorie
Sofortige Löschung	auf Verlangen des Betroffenen, soweit keine Rechts- oder Vertragsgrundlage besteht
6 Monate	nach Beendigung der Zweckbindung (z. B. Mietinteressenten, ohne dass ein Vertrag zu Stande gekommen ist, Frist ab Mietgesuch) Schufa- und sonstige Bonitätsauskünfte, Leistungsbescheide von Behörden, Einkommensnachweise
1 Jahr	für Vertragsverhältnisse, die nur ein Jahr gültig sind bzw. bei denen nach einem Jahr der Zweck entfällt (bspw. Mietinteressentenbogen, Mieterselbstauskunft)
3 Jahre	nach Vertragsende zum Jahresende gemäß § 195 BGB = Regelmäßige Verjährungsfrist (wenn keine neuen Ansprüche entstanden sind)
6 Jahre	Verträge, wie Miet- und Pachtverträge (nach Vertragsende) Geschäftsbriefe (Briefe, E-Mails, Faxe, etc.), Mahnungen
10 Jahre	Steuer- und handelsrechtliche Geschäftsunterlagen, z.B. Inventare, Jahresabschlüsse, Buchungsbelege, Handels- und Geschäftsbriefe, Rechnungen (auch für Betriebskosten) nach Vertragsende zum Jahresende nach § 257 HGB und § 147 AO. (Endgültiges Löschen aller personenbezogenen Daten, z. B. Debitorendaten), gilt auch für Mieterakte
30 Jahre	bei titulierten Forderungen nach dem Ende des Vertragsverhältnisses, Zahlungs- und Räumungstitel, Zwangsvollstreckungsbescheide

Tabelle 4: Ausgewählte Aufbewahrungsfristen
Quelle: DOMUS Consult Präsentation „Löschen nach Konzept“ 2021, eigene Recherche

Daneben sind die branchen- und anwendungsspezifischen Vorschriften, bspw. aus dem Genossenschaftsgesetz, zu beachten.

3. Ausgewählte Handlungsempfehlungen für Wohnungsunternehmen

1. Grundsätzliches zur Datenverarbeitung

Folgende Fragen sollte sich das Wohnungsunternehmen in Bezug auf die Verarbeitung pbD regelmäßig stellen:

- Welche pbD dürfen/können/müssen erfasst werden?
- Wie liegen die pbD vor? Analog und/oder digital?
- Welche pbD werden rückstandslos gelöscht, welche anonymisiert oder pseudonymisiert?
- Wie werden die pbD gelöscht? Manuell und/oder automatisiert?
- Welche Ausnahmen und Spielräume gibt es, pbD länger aufzubewahren?

2. Erstellung eines Löschkonzepts – aber wie?

Für die Erstellung eines Löschkonzepts sollten folgende Schritte berücksichtigt werden:

Schritt 1: IT-Systeme, digitale und analoge Datenablagen, in den pbD verarbeitet/aufbewahrt werden, identifizieren

Schritt 2: Datenarten bestimmen, die in den Ablagesystemen verarbeitet werden

Schritt 3: Datenarten zu Datenkategorien zusammenfassen

Schritt 4: Konkrete Fristen festlegen

Schritt 5: Datenkategorien den Löschklassen zuordnen

Schritt 6: Löschregeln für die Datenkategorien definieren

Schritt 7: Konkretes Umsetzungsvorgehen festlegen

Schritt 8: Verantwortliche für das konkrete Löschen benennen (nicht der Löschbeauftragte!)

Schritt 9: Löschabläufe dokumentieren

In diesem Zusammenhang wird auf die **Anlage 1** „Checkliste IT“ verwiesen, welche Umsetzungsvorgaben für verschiedene Löschobjekte gibt.

3. Prämisse Datenminimierung „Weniger ist mehr“

Bereits in Art. 5 Nr. 1c DSGVO wird die Datenminimierung festgelegt. So müssen pbD „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“.

Je weniger Daten von vornherein erfasst und gespeichert werden, desto weniger Daten müssen später geprüft und gelöscht werden. Daher empfiehlt sich die Datenerhebung nach dem Motto „weniger ist mehr“ zu leben.

Regelmäßig die Frage stellen:

- Welche Daten sind vertraglich erforderlich?
- Welche Informationen sind für die Wohnung relevant/interessant?

4. Verhältnismäßigkeit und Risikoabschätzung

Stellen Sie sich die Frage, ob dieses Dokument oder diese Information mit pbD erhoben werden muss. Welcher Zweck wird mit der Erhebung und Speicherung der Information verfolgt? Umso mehr Daten im Laufe der Vertragsbeziehung angesammelt werden, umso mehr Daten und Dokumente müssen nach Ablauf der Speicherfristen geprüft und gelöscht werden.

Nehmen Sie eine Risikoabschätzung vor, um festzustellen, welches Risiko maximal besteht, wenn die pbD nicht erhoben werden oder es zu einem Datenschutzvorfall mit erhobenen und nicht gelöschten pbD kommt. Beurteilen Sie realistisch und wirtschaftlich, ob es sich um seltene Einzelfälle handelt, dass eine bestimmte Mieterinformation auch nach mehr als zehn Jahren noch relevant ist. Handeln Sie stets nach der Prämisse Datenminimierung.

5. Prüfung von Dokumenten mit pbD

Die Löschfristen bestehen für Dokumente mit pbD und nicht für Vorgänge. Daher wird empfohlen ausgewählte Teilbereiche eines Dokuments zu erfassen, um die Prüfung des Dokuments (bspw. Personalausweis, Reisepass, Gehaltsnachweis) nachzuweisen und damit auf die Kopie oder den Scan des Dokuments zu verzichten. Diese Empfehlung gilt gleichermaßen für den Abschluss von Mietverträgen und Beschäftigungsverhältnissen.

Praxistipp: Personalausweis und Gehaltsnachweise von Mietinteressenten

Personalausweise und Gehaltsnachweise sollten nicht kopiert oder gescannt werden. Auch wenn diese Dokumente dem Wohnungsunternehmen analog oder digital zugehen, sollten sie nicht erst im System gespeichert werden, sondern schnellstmöglich rückstandslos gelöscht werden.

Empfohlen wird stattdessen eine Checkliste, auf der die Vorlage gegenüber dem Unternehmen und Plausibilitätsprüfung der Dokumente durch den Mitarbeitenden bestätigt wird. Konkrete Inhalte dieser Dokumente, wie Ausweisnummer oder Ablaufdatum können problemlos notiert und gespeichert werden.

6. Datenkategorien festlegen

Welche pbD von welchen Interessengruppen werden gespeichert und verarbeitet? Es können bspw. folgende Datenkategorien unterschieden werden:

- Mietinteressenten
- Mieter und Mitglieder
- Mitarbeitende und Bewerber
- Kontrollgremien, bspw. Aufsichtsrat
- Kreditoren und Debitoren
- Weitere Kategorien

Klassifizieren Sie die pbD, die aufgenommen und gespeichert werden sollen. Legen Sie Regeln fest zu pbD, die abgefordert wurden und erforderlich sind (→ notwendige pbD), und pbD sowie Dokumente, die freiwillig übermittelt wurden (→ optionale pbD). Auch diese Informationen sollten nicht länger und nicht mehr als nötig gespeichert und verarbeitet werden.

Checklisten für die Interessentenverwaltung (**Anlage 2**) und die Mieterverwaltung (**Anlage 3**) finden sich im Anhang.

7. Doppelstrukturen vermeiden

Werden Dokumente oder ganze Akten digitalisiert, ist darauf zu achten, dass alle zugehörigen Dokumente unabhängig des Dateityps (Vertrag, Brief, Akten-, Telefonnotiz, Fax, etc.) digitalisiert und zentral gespeichert werden, um eine 1:1-Abbildung der Papierakte zu erhalten.

Praxistipp: Sammel-pdf´s vermeiden

Bei der Digitalisierung von Mieterakten und Vertragsanlagen ist darauf zu achten, dass thematisch abgrenzbare Dokumente einzeln eingescannt werden. Diese können später per Schlagwortsuche schneller aufgefunden und in Löschautomatismen aufgenommen werden. So können Löschfristen der unterschiedlichen Daten-kategorien leicht eingehalten werden.

8. Nachhaltige und effiziente Datenverarbeitung

Digital eingegangene Dokumente sollten auch digital archiviert werden. Vermeiden Sie zusätzliche Ausdrucke, um später doppelte Löschvorgänge für analog und digital abgelegte pbD Daten zu vermeiden.

9. Einwilligungen und Widerruf

Einwilligungen zur Datenverarbeitung müssen schriftlich oder elektronisch erfolgen (Art. 4 Nr. 11 DSGVO). Einwilligungen sind nur rechtskräftig, wenn diesen widerrufen werden kann. Achten Sie daher auf das Vorhandensein des Widerrufspassus.

10. Einhaltung von Löschfristen

Halten Sie sich an gesetzliche Löschfristen. Sind keine starren Fristen vorgegeben, beschreiben Sie den Geschäftsprozess und argumentieren die von Ihnen festgelegten Löschfristen.

Eine Übersicht zu ausgewählten Aufbewahrungsfristen ist in **Abschnitt 2.6** zusammengestellt.

Praxistipp: Betriebskostenabrechnung und Schriftverkehr[1]

Daten, die für die Betriebskostenabrechnung nötig sind, müssen mind. bis zum Ablauf der Einwendungsfrist (§ 556 Abs. 3 BGB), bedeutet zwölf Monate nach Zustellung der Abrechnung aufbewahrt werden.

Daten, die Vermieteransprüche betreffen, sollten bis zur Verjährungsfrist nach § 195 BGB, also drei Jahre, aufbewahrt werden.

11. Löschung dokumentieren

Die Löschung von Dokumenten nach Ablauf der Löschfristen muss protokolliert werden.

Eine Vorlage für ein Löschprotokoll findet sich in **Anlage 4**.

12. Regelmäßigkeit hilft

Etablieren Sie Unternehmensprozesse, bei denen regelmäßig die Einhaltung der Löschfristen geprüft wird. Legen Sie fest, wer für die Löschung verantwortlich ist.

Praxistipp: Konsequente Prüfung

Jedes Mal, wenn die Mieterakte geöffnet wird, sollte geprüft werden, ob pbD gelöscht werden müssen bzw. können, um hierdurch Schritt für Schritt analoge und digitale Mieterakten zu bereinigen.

[1] Vgl. Schmidt/Schweißguth/Hoffmann/Hummel (2018): Datenschutz in der Wohnungswirtschaft, Haufe Group, 1. Auflage, S. 128.

13. Software und IT-Verträge

Verwendete und geplante Software sollten darauf geprüft werden, ob erhobene pbD rückstandslos gelöscht werden können oder technisch eine Anonymisierung oder Pseudonymisierung möglich ist.

Beim IT-Dienstleister sollten das Lösch- und Sperrkonzept sowie die Standorte von Aktiv- und Passivservern (Backupservern) erfragt werden.

Es sollten nur Verträge mit Softwareanbietern abgeschlossen werden, die zusichern, dass pbD gelöscht werden können. Auftragsverarbeitungsvereinbarungen (kurz AVV) mit Dienstleistern sollten genau geprüft, ggf. nachverhandelt werden.

14. Sensibilisierung und Schulung aller Beteiligten

Mitarbeitende sollten regelmäßig – alle ein bis zwei Jahre – geschult werden. Schulungen sollten praxisnah sein und können auch mal durch ungewöhnliche Formate umgesetzt werden. Mitarbeitenden muss bewusst sein, dass sie eine Mitwirkungspflicht bei der Umsetzung des Löschkonzepts haben.

Wichtig sind regelmäßige Wiederholungen, damit die Themen immer wieder ins Gedächtnis gerufen werden. Hierbei sollte darauf geachtet werden alle Mitarbeitenden, also auch Azubis, Praktikanten oder andere kurzzeitig Beschäftigte, über die Regeln im Unternehmen aufzuklären. Mehr Verständnis und Nachvollziehbarkeit bei den Mitarbeitenden wird erreicht, wenn die dahinterliegenden Prozesse und Sinnhaftigkeit erklärt werden.

Hierzu bieten sich folgende Formate an:

a) Regelmäßige Präsenzschulungen bspw. mit dem (externen) Datenschutzbeauftragten
b) Anlassbezogene Schulungen, bspw. nach Auftreten eines Datenschutzvorfalls
c) Regelmäßige Sensibilisierung über Online Lernvideo Plattformen
d) Phishing bzw. Social Hacking Aktionen, um mögliche Situationen aus der Praxis zu testen
e) Persönliche Gespräche mit Mitarbeitenden führen
f) Rollenspiele durchführen, bei dem sich Mitarbeitende in die Rolle der Mieter versetzen

Praxistipp: Praxisnahe Beispiele in Schulungen

Schulungsinhalte und Beispiele mit dienstlichem sowie privatem Bezug können und sollten kombiniert werden, um einen höheren Lerneffekt zu erzielen. Realistische Beispiele wirken nachhaltiger.

Mindestens genauso wichtig, wie die Schulung der Belegschaft, ist die Sensibilisierung und Beurteilung der Relevanz bei den Führungskräften. Ist den Vorständen und Geschäftsführern die Bedeutung der Datenspeicherung und -löschung bewusst, können Geschäftsprozesse schneller optimiert werden.

15. Partizipation der Mitarbeitenden

Bei der Festlegung von nicht gesetzlich vorgeschriebenen Löschfristen sollten Fachabteilungen und Mitarbeitende aktiv einbezogen werden. Durch die Einbindung der Belegschaft in den Prozess steigt die Einsicht und Einhaltung der selbst mitgestalteten Verfahren und Regelungen. Mitarbeitende haben für ihren Verantwortungsbereich oft gute Ideen und Problemlösungsvorschläge. Zuhören und in Veränderungen einbinden, erhöht die Akzeptanz und Zufriedenheit bei der Belegschaft.

Praxistipp: Tag des Löschens

Führen Sie einen konkreten Tag ein, an dem alle Mitarbeitenden aufgerufen sind die pbD in ihrem jeweiligen Verantwortungsbereich zu löschen, die gemäß Löschfrist gelöscht werden müssen.
Hierzu eignet sich bspw. der **Europäische Datenschutztag, 28. Januar**. Der Aktionstag für den Datenschutz wurde 2007 vom Europarat ins Leben gerufen.

16. Einbindung des Betriebsrat

Bei Vorhandensein eines Betriebsrates im Unternehmen sollte dieser frühzeitig und regelmäßig in die Prozesse und damit in die Umsetzung des Löschkonzepts involviert werden.

17. Funktions-Postfächer nutzen

Nutzen Sie neben personalisierten E-Mail-Adressen auch separate E-Mail-Postfächer für bestimmte Zielgruppen (bspw. Mieter, Bewerber) und Geschäftsbereiche bzw. Abteilungen (bspw. vermietung@, reparatur@, vorstand@).

Der Zugriff auf die E-Mail-Postfächer kann für mehrere Personen eingerichtet werden und lässt sich schnell aktivieren und deaktivieren.

Weiterhin können sensible Informationen direkt an den Personenkreis gesendet werden, der auf diese Postfächer Zugriff hat. Filter- und Löschaktivitäten können hierdurch erleichtert werden.

Praxistipp: Eigenes Bewerber-Postfach

Legen Sie ein E-Mail-Postfach für Bewerber (z.B. bewerbung@muster-wu.de) an. Teilen Sie den Bewerbern unverzüglich die Datenschutzhinweise mit und löschen nach Ablauf der Aufbewahrungsfrist die Bewerberdaten.

18. E-Mail-Archivierung und -Aufbewahrung

Geschäftsvorfallsrelevante E-Mails sollten umgehend archiviert werden. Bei Nutzung einer E-Mail Archivierungssoftware können Löschregeln eingerichtet werden, die automatisiert die Löschung nach Ablauf der Löschfrist übernehmen. Digitale und analoge Geschäftsbriefe (auch E-Mails) müssen sechs Jahre aufbewahrt werden.

Die Mitarbeitenden sollten Kenntnis über und Zugriff auf die Datenschutzleitlinie und -richtlinie des Unternehmens haben und regelmäßig an die Regelungen erinnert werden, bspw. im Rahmen der Schulungen und Sensibilisierungsmaßnahmen.

Praxistipp: Automatisiertes Löschen

Legen Sie einen Zeitpunkt fest, nach dem nicht archivierte und damit nicht für Geschäftsvorfälle relevante E-Mails in personalisierten Postfächern automatisch gelöscht werden, bspw. nach zwei Jahren.

Damit werden alle Mitarbeitenden angehalten, ihren Archivierungspflichten nachzukommen und die E-Mail-Postfächer bleiben übersichtlich. Zudem wird der Speicherplatz auf den Servern hierdurch nicht überfrachtet.

19. Auf IT-Systeme und Berechtigungsstrukturen achten

Es wird empfohlen für die IT-Systeme (bspw. MS365, ERP-Systeme, DMS, etc.) ein Rollen- und Rechtekonzept zu erarbeiten und die Benutzer definierten Gruppen zuzuordnen. Damit können nach Ausscheiden oder Veränderungen der Verantwortungsbereiche die Mitarbeitenden sauber zugeordnet oder Zugriffsberechtigungen angepasst werden.

Praxistipp: ERP-Systeme

In ERP-Systemen sollten Benutzer nicht gelöscht, sondern pseudonymisiert werden, da sonst Verknüpfungen ungewollt entfernt werden.

4. Abkürzungsverzeichnis

Abkürzung	Bezeichnung
AGG	Allgemeines Gleichbehandlungsgesetz
AO	Abgabenordnung
Art.	Artikel
AVV	Auftragsverarbeitungsvereinbarung
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
DMS	Dokumentenmanagementsystem
DSB	Datenschutzbehörde
DSGVO	Datenschutz-Grundverordnung
EU	Europäische Union
GdW	GdW Bundesverband deutscher Wohnungs- und Immobilienunternehmen e. V.
GWW	Geldwäschegesetz
HGB	Handelsgesetzbuch
pbD	Personenbezogene Daten
KWG	Kreditwesengesetz
vtw	Verband Thüringer Wohnungs- und Immobilienwirtschaft e.V.

5. Glossar

Begriff	Erläuterungen
Aufbewahrungsfrist	Frist, für deren Zeitraum eine Datenkategorie nach rechtlichen Vorgaben beim Verantwortlichen verfügbar sein muss
Auftragsverarbeiter	Agiert ausschließlich weisungsabhängig im Auftrag des Verantwortlichen (Art. 4 Nr. 8, Art. 28 DSGVO)
Datenarten	Für Wohnungsunternehmen typische Datenarten sind bspw.: • Stammdaten (Anschrift, Kontaktdaten, usw.) von Mietern, Miet-/Kaufinteressenten, Mitgliedern, Mitarbeitenden • Vertragsdaten • Abrechnungsdaten • Verbrauchsdaten (Energie, Wasser, Müll) • Buchhaltungsdaten (Zahlungsströme, Inkasso, Buchungsbelege, etc.)
Datenkategorien	Zusammenfassung von Datenarten in Oberbegriffe
Datenschutzbeauftragter	Wirkt auf die Anwendung und Umsetzung des Löschkonzepts im Unternehmen hin
Löschbeauftragter	Verantwortlich für die Definition der Löschregeln und die Prüfung der Umsetzung des Löschkonzepts
Löschfrist	Zeitspanne, nach der die Daten (in der Regel) gelöscht werden sollen, unter Beachtung von vertraglichen und rechtlichen Aufbewahrungsfristen
Löschklasse	Kombination aus einer Standardlöschfrist und einem abstrakten Startzeitpunkt für den Fristlauf
Löschregel	Kombination aus Löschfrist und konkreter Bedingung für den Startzeitpunkt des Fristlaufs. Eine Datenart = eine Löschregel!

Begriff	Erläuterungen
Mitarbeitende	Führen das Löschen lokal gespeicherter Daten auf Endgeräten und E-Mails, in Anwendungssystemen (Anwendungsverantwortliche) und IT-Systemen (Administratoren) durch
Regellöschfrist	Summe aus Vorhaltefrist und datenschutzrechtlich vertretbarer Frist bis zur Löschung definiert die längst mögliche Frist bis zur Löschung. Nach Ablauf der Frist müssen die Daten gelöscht werden.
Standardlöschfrist	Festgelegte Löschfristen, die sich anhand der einschlägigen Rechtsvorschriften und den bestehenden vertraglichen oder gesetzlichen Regelungen ableiten lassen, bspw. DSGVO, BDSG, HGB, AO, AGG, GwG, KWG
Startzeitpunkt	Beginn der Regellöschfrist. Es treten drei Typen von Startzeitpunkten auf: ab Erhebung, ab dem Ende eines Vorgangs bzw. der Beziehung zum Betroffenen und Individuell.
Verantwortlicher	Legt Zweck und Mittel der Verarbeitung fest, verpflichtet sich als Verantwortlicher zur rechtskonformen Löschung pbD (Art. 4 Nr. 7, Art. 24 ff. DSGVO)
Vorhaltefrist	Zeitraum, innerhalb dessen pbD auf Grund der betrieblichen Anforderungen oder gesetzlicher Aufbewahrungspflichten mindestens verfügbar zu halten sind

Anlage 1: Checkliste IT

IT-Systeme

1. Ausgangssituation:
   ERP-System & Module, Archivsystem / DMS, Controllingsystem, E-Mailsystem, Zeiterfassung, Mobile Device Management, Cloudsysteme

2. Identifikation:
   Erhebung IT-Systeme mittels Interviews, VVT

3. Behandlung zum Löschen:
   Herstellerspezifische Lösung?
   Manuell oder automatisch?
   Löschen oder anonymisieren?

Filesystem

1. Ausgangssituation:
   unstrukturierte Ablage, verschiedene Formate (docx, xlsx, pdf, etc.), nur Mitarbeitende kennen die Ablage

2. Identifikation:
   Erhebung von Filename, Ablageort, Zweck der Verarbeitung über Mitarbeitende

3. Behandlung zum Löschen:
   Notwendigkeit?
   Datenbereinigung File-Verzeichnis?
   Manuell oder automatisch?
   Umbenennung Dateien?
   Reorganisation File-Ablage?

Papierdokumente

1. Ausgangssituation:
   strukturierte Ablage in Aktenordnern in Archivräumen und Büros

2. Identifikation:
   Sichtung der Aktenstruktur, Erhebung von Dokumenten mit pbD mit Namen, Ablageort, Zweck der Verarbeitung

3. Behandlung zum Löschen:
   Vernichtung von Dokumenten/ Akten möglich?
   Neuklassifizierung Dokumente?
   Reorganisation Archivstruktur?

E-Mails

1. Ausgangssituation:
   jede E-Mail enthält pbD, Mails werden im Postfach lange aufbewahrt, oftmals ins Filesystem verschoben

2. Identifikation:
   Sichtung & Prüfung durch Mitarbeitende zur Feststellung der Aufbewahrungspflicht

3. Behandlung zum Löschen:
   Organisationsrichtlinie?
   Grundsätzlich E-Mails nach x Jahren löschen?
   Einführung revisionssicheres Archiv?

Abbildung 2: Checkliste IT für Umsetzungsvorgaben bei ausgewählten Löschobjekten
Quelle: vgl. Domus Consult Präsentation „Löschen nach Konzept“ 2021

Anlage 2: Muster-Checkliste für Interessentenverwaltung

1. Festlegung der Löschfristen im Verzeichnis der Verarbeitungstätigkeiten für die Interessentenverwaltung

Nach Art. 30 DSGVO ist jedes Unternehmen verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Daraus ergibt sich, dass entsprechend Absatz 1 f die vorgesehenen Fristen für die Löschung der Daten, hier speziell für die Interessentenverwaltung, zu vermerken sind, welche die Grundlage für die Anwendung des Löschkonzeptes bilden.

Verarbeitungsverzeichnis Interessentenverwaltung:

- Welche personenbezogenen Daten werden in der Interessentenverwaltung bearbeitet?
- Wer ist verantwortlich für die Verarbeitung der Daten?
- Welchem Zweck dient die Verarbeitung der Daten?
- Welche Daten sind betroffen?
- Welche Fristen für die Löschung sind festgelegt?
- Welche Aufbewahrungsfristen sind gesetzlich vorgegeben?

2. Beendigung der Zweckbindung für die Datenspeicherung von Interessentendaten

Gemäß der DSGVO ist die Zweckbindung der Daten einzuhalten. Ist diese nicht mehr vorhanden, dann müssen die Daten gelöscht werden (Art. 5 und Art. 17 DSGVO).

Dienstanweisung/Organisationsanweisung/Arbeitsanweisungen:

- Unter welchen Bedingungen/Voraussetzungen sind die personenbezogenen Interessentendaten zu löschen? (z. B. Vertrag ist nicht zu Stande gekommen, Ablauffrist)
- Welche Daten werden gelöscht? (z. B. alle Daten zum Interessenten)
- Wie ist mit den Interessentenbogen umzugehen? (z. B. 6 Monate Aufbewahrung, individuell vereinbarte Ablauffrist mit dem Interessenten)
- Mit welcher Regelmäßigkeit werden die elektronischen Daten des Interessenten gelöscht? (z. B. monatlich, quartalsweise)

3. Organisation der Löschung von Interessentendaten

- Wer ist für die Löschung welcher Daten verantwortlich?
- Wer ist für das Vernichten der Papierdokumente (z. B. Interessentenbogen) verantwortlich?
- Wer kontrolliert diesen Prozess?
- Welche Unterlagen sind notwendig?
- Nach welchen Dienstanweisungen/Organisationsanweisungen sollten sich die Mitarbeitenden orientieren?
- Welche wesentlichen Gesetzlichkeiten sind zu beachten?
- Welche Ressourcen werden benötigt?
- Welche Berechtigungen sind notwendig?
- In welchem Rhythmus ist die Löschung durchzuführen?

4. Festlegungen der Arbeitsschritte für die Löschung von Interessentendaten

- Falls Interessentenbogen in Papierform vorhanden sind, sind diese monatlich entsprechend der festgelegten Ablauffrist zu prüfen und zu vernichten.
- Während des Arbeitsprozesses sind Interessenten mit entsprechenden Ablehnungsgründen (z. B. bereits Wohnung gefunden, negative Schufa, Mietschulden, mietwidriges Verhalten, möchte nicht mehr umziehen) zu kennzeichnen.
- Monatlich sollte für diese inaktiv gekennzeichneten Interessenten die Löschung der Daten automatisiert oder manuell erfolgen.
- Einzelne aktive Interessenten, bei denen der Mietvertrag nicht zu Stande gekommen ist, sind jederzeit von den Bearbeitern manuell zu entfernen.
- Eine sofortige Löschung ist vorzunehmen, wenn der Interessent es sofort verlangt.
- Regelmäßig (z. B. monatlich, quartalsweise) ist eine automatisierte elektronische Löschung der Interessentendaten vorzunehmen, bei denen die vereinbarte oder festgelegte Ablauffrist verstrichen ist.

5. Nachweisführung über die Löschung der Interessentendaten und Kontrollpflicht

- Jede Löschung, ob automatisiert oder manuell, wird in einem Protokoll festgehalten und nachgewiesen.
- Erfasst werden die Interessenten-ID, das Löschdatum und der Mitarbeiter, der die Löschung vorgenommen hat.
- Der Löschprozess ist regelmäßig durch die Geschäftsleitung im Rahmen des internen Kontrollsystems zu kontrollieren.

Anlage 3: Muster-Checkliste für Vertrags- bzw. Mieterverwaltung

1. Festlegung der Löschfristen im Verzeichnis der Verarbeitungstätigkeiten für die Vertragsverwaltung

Nach Art. 30 DSGVO ist jedes Unternehmen verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Daraus ergibt sich, dass entsprechend Absatz 1 f die vorgesehenen Fristen für die Löschung der Daten, hier speziell für die Mieterverwaltung, zu vermerken sind, welche die Grundlage für die Anwendung des Löschkonzeptes bilden.

Verarbeitungsverzeichnis Vertragsverwaltung:

- Welche personenbezogenen Daten werden in der Vertragsverwaltung bearbeitet?
- Wer ist verantwortlich für die Verarbeitung der Daten?
- Welchem Zweck dient die Verarbeitung der Daten in der Vertragsverwaltung?
- Welche Daten sind betroffen?
- Welche Fristen sind für die Löschung festgelegt?
- Welche Aufbewahrungsfristen sind gesetzlich vorgegeben?

2. Beendigung der Zweckbindung für die Datenspeicherung von Mieterdaten

Gemäß der DSGVO ist die Zweckbindung der Daten einzuhalten. Ist diese nicht mehr vorhanden, dann müssen die Daten gelöscht werden (Art. 5 und Art. 17 DSGVO).

Dienstanweisung/Organisationsanweisung/Arbeitsanweisungen:

- Unter welchen Bedingungen/Voraussetzungen sind die personenbezogenen Mieterdaten zu löschen? (z.B. Definieren der unterschiedlichen Löschfristen für die Vertragsverhältnisse, Definieren von Start und Ende der Aufbewahrung, Grund der Löschung)
- Welche Daten werden gelöscht? (z.B. Name, Vorname, Titel, Suchbegriff, Debitorenname)
- Welche Daten werden pseudonymisiert? (z.B. Name, Vorname, Titel, Suchbegriff, Debitorenname)
- Wie ist mit den Papierunterlagen der Mieter umzugehen?

3. Organisation der Pseudonymisierung und Löschung von Daten der Vertragsverwaltung

- Wer ist für die Löschung welcher Daten verantwortlich?
- Wer ist für das Vernichten der Papierdokumente verantwortlich?
- Wer kontrolliert diese Prozesse?
- Welche Unterlagen sind notwendig?
- Nach welchen Dienstanweisungen/Organisationsanweisungen sollten sich die Mitarbeitenden orientieren?
- Welche wesentlichen Gesetzlichkeiten sind zu beachten?
- Welche Ressourcen werden benötigt?
- Welche Berechtigungen sind notwendig?
- Sollten zusätzliche Berechtigungen zum Löschen von Daten über eine begrenzte Frist freigeschalten werden?
- In welchem Rhythmus ist die Löschung/Pseudonymisierung durchzuführen?

4. Festlegungen der Arbeitsschritte für die Löschung von Daten in der Vertragsverwaltung

- Auswertung aller ehemaligen Mietverhältnisse „bis Jahr“ entsprechend der Festlegung (Punkt 2) sowie z.B. auch Daten, bei denen kein Vertrag zu Stande gekommen ist
- Übersicht aller wesentlichen Stammdaten zum ehemaligen Mietverhältnis als Arbeitsgrundlage für die verantwortlichen Mitarbeitenden und Teams
- Prüfung des Mietverhältnisses - Kriterien: Saldo = NULL, kein Mahnkennzeichen, kein Rechtsfall, keine Pfändung, kein Mahnbescheid
- Prüfung in der Kautionsverwaltung auf vollständige Abrechnung des Kautionskontos
- Prüfung, dass kein Inkassoverfahren vorliegt
- Prüfung elektronisch abgelegter Dokumente im Archiv und der dazugehörigen Papierakten
- Pseudonymisierungs- oder Löschprozess im ERP-System für die Kontakte und Debitoren durchführen
- Löschung des dazugehörigen Kautionskontos
- Löschung der Dokumente im elektronischen Archiv und Vernichtung der Dokumente des Papierarchivs

5. Nachweisführung über die Pseudonymisierung bzw. Löschung der Mieterdaten und Kontrollplicht

- Protokollierung aller Pseudonymisierungen und Löschungen – nachvollziehbare Übersicht / Auswertung der Datennachweise - Information, wann ist welcher Mieter (Kontakt, Debitor) von wem im ERP-System pseudonymisiert bzw. gelöscht worden
- Regelmäßige Prüfungen der Ordnungsmäßigkeit der Durchführung des Löschprozesses durch die Geschäftsleitung sind im Rahmen des internen Kontrollsystems durchzuführen

Anlage 4: Muster Löschprotokoll

Muster eines Löschprotokolls mit **Beispielangaben**

Verantwortliches Unternehmen:	WBG Muster eG
Löschzeitraum:	01.01.20XX – 31.12.20XX
☒ Anwendung:	Aareon Wodis Sigma
☐ Datei (mit Pfadangabe):	
☐ Dokument (mit Ortsangabe):	
Grund der Löschung:	Durchführung nach Ablauf Löschfrist und Beendigung aller Geschäftsbeziehungsarten
Löschung durchgeführt für [Datenkategorien]:	Mieter, Mitglieder
Datensätze [Anz.]	X.XXX
Datum der Löschung:	im Zeitraum vom XX.XX.20XX bis XX.XX.20XX
Löschung durchgeführt von [Löschverantwortlicher]:	
Datum der Prüfung der Löschung durch Löschbeauftragten:	
Prüfung der Löschung durchgeführt von [Löschbeauftragter]:	
Anmerkungen zur Löschung:	Löschvorgang erfolgreich
Anlagen zur Löschung:	Wodis „Löschübersicht (DSGVO)“

Ort, Datum

Ort, Datum

_____

Löschverantwortlicher

_____

Löschbeauftragter