RICHTLINIE ZUM DATENSCHUTZ

der

Allgemeinen Wohnungsbaugenossenschaft „Eisenach“ eG

Geltungsbereich:	Alle Unternehmensbereiche
Revisionsnummer / DocID:	080202-01
Datum der Herausgabe:	06.11.2025
Erarbeitung:	GOL/WAT/Herr Schwanitz
Freigabe am: / durch:	10.11.25 / Vorstand

Datum	Bearbeiter	Inhalt
13.05.2024	GOL/WAT	Konzeptionelle Erarbeitung
30.10.2025	GOL/WAT	Besprechung mit dem DSB
05.11.2025	WAT	Anpassungen/Aktualisierungen
06.11.2025	GOL/WAT	Finalisierung und Vorlage für Vorstand

„EISENACH“eG

Inhaltsverzeichnis

1 Organisation

Unternehmen

Unternehmen:	AWG „Eisenach“ eG, vertreten durch den Vorstand
Standort:	Stregdaer Allee 44A, 99817 Eisenach
Datenschutzkoordination:	Herr David Golling, Frau Heike Wartmann AWG „Eisenach“ eG datenschutz@awg-eisenach.de
Externer Datenschutzbeauftragter:	DOMUS Consult Wirtschaftsberatungsgesellschaft mbH Schornsteinfegergasse 13 14482 Potsdam Herr Ronny Schwanitz 0172 3094204 schwanitz@domusconsult.de

2 Gegenstand der Datenschutzrichtlinie

Die Verarbeitung personenbezogener Daten (pbD) spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen operativen Funktionen und Aufgaben basieren auf einer Verarbeitung pbD. Die von der AWG „Eisenach" eG, vertreten durch den Vorstand verarbeiteten und genutzten personenbezogenen Daten sowie die Nutzung unserer IT-Systeme und physischen Ablagen in allen Bereichen sind in ihrer Verfügbarkeit, Vertraulichkeit und Integrität so zu sichern, dass die Anforderungen der DS-GVO und des BDSG eingehalten werden.

3 Gültigkeit / Inkrafttreten

Diese Datenschutzrichtlinie tritt mit Wirkung vom 01.11.2025 mit dem Revisionsstand 1.0 in Kraft.

4 Ziel der Datenschutzrichtlinie

Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Kunden- und Geschäftsbeziehungen und die Reputation der AWG „Eisenach" eG, vertreten durch den Vorstand im Innen- und Außenverhältnis. Diese Datenschutzrichtlinie beinhaltet die Vorgaben zum Umgang mit personenbezogenen Daten bei der AWG „Eisenach" eG, vertreten durch den Vorstand.

Diese Datenschutzrichtlinie verpflichtet alle Beschäftigten zur Einhaltung der hier festgelegten Anforderungen zur Aufrechterhaltung des Datenschutzes.

5 Geltungsbereich der Datenschutzrichtlinie

Die Datenschutzrichtlinie gilt für alle beschäftigten Personen, auszubildenden Personen und Aushilfen, mit denen die AWG „Eisenach" eG, vertreten durch den Vorstand Verträge zur Leistungserbringung vereinbart hat, im Folgenden Beschäftigte genannt.

Die Datenschutzrichtlinie erstreckt sich auf sämtliche Prozesse, bei denen personenbezogene Daten verarbeitet werden. Das bezieht sich sowohl auf das Unternehmen AWG „Eisenach" eG als auch auf das Tochterunternehmen „Haus und Wohnen Eisenach GmbH" (HWE), sowie die durch Geschäftsbesorgungsvertrag gebundenen Wohnungsunternehmen.
Die Verarbeitung anonymisierter Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegt grundsätzlich nicht dieser Datenschutzrichtlinie.

6 Prinzipien für die Verarbeitung personenbezogener Daten

Das Unternehmen berücksichtigt bei der Planung, Einführung und während des Ablaufs von Prozessen nachfolgende Prinzipien:

1. Die Verarbeitung personenbezogener Daten erfolgt stets auf rechtmäßige Weise, für den Betroffenen transparent, sowie nach den Grundsätzen von „Treu und Glauben“.
2. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich für festgelegte, eindeutige und legitime Zwecke („Zweckbindung“).
3. Die Verarbeitung der personenbezogenen Daten erfolgt für alle Betroffenen transparent, indem diese vor der Verarbeitung über den Umgang mit ihren Daten informiert werden.
4. Die Erhebung und Verarbeitung personenbezogener Daten erfolgt stets im für die Durchführung des Prozesses minimal notwendigen Umfang.
5. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden.
6. Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, werden gelöscht.
7. Personenbezogene Daten werden regelmäßig auf Korrektheit, Vollständigkeit und Zweckbindung geprüft.
8. Personenbezogene Daten werden durch angemessene technische und organisatorische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie versehentlichen Verlust, vor Veränderung oder Zerstörung gesichert.

7 Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist rechtlich nur zulässig, wenn ein Erlaubnistatbestand entsprechend Artikel 6 DS-GVO oder §26 BDSG vorliegt.

Durch den Verantwortlichen einer Verarbeitungstätigkeit muss bei Einführung das Vorliegen eines entsprechenden Erlaubnistatbestandes geprüft werden. Das Ergebnis der Prüfung ist zu dokumentieren und durch den externen Datenschutzbeauftragten zu bestätigen. Die Verarbeitungstätigkeit ist im Verzeichnis der Verarbeitungstätigkeiten (VVT) mitaufzunehmen.

Die wichtigsten Erlaubnistatbestände sind:

7.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. In der Vertragsanbahnungsphase ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Nutzungsverträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten, auf die Verwendung der Daten beschränkt, die der Betroffene mitgeteilt hat. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten.

7.2 Datenverarbeitung auf Basis einer Einwilligung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z. B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Die Erteilung muss dokumentiert werden.

Der Inhalt einer Einwilligung sollte auch immer einen Hinweis auf das Widerrufsrecht enthalten: *„Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Alle bis zum Zeitpunkt des Widerrufs erfolgten Verarbeitungen bleiben jedoch vom Widerruf unberührt“.*

7.3 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

7.4 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der AWG „Eisenach“ eG, vertreten durch den Vorstand erforderlich ist. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen.

Soll eine Verarbeitung auf Basis einer Interessenabwägung durchgeführt werden, so ist sowohl das berechtigte Interesse als auch das Risiko, was für den Betroffenen entsteht, zu beschreiben und dem externen Datenschutzbeauftragten zur Prüfung zu übermitteln. Der Start der Verarbeitung darf erst nach Freigabe durch den externen DSB erfolgen.

7.5 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind.

Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern nur in dem Umfang und Zeitrahmen verarbeitet werden, die es ermöglichen, eine Eignung festzustellen.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein. Ergänzt werden kann dies durch den Abschluss von Betriebsvereinbarungen.

8 Verzeichnis von Verarbeitungstätigkeiten

Die AWG „Eisenach“ eG, vertreten durch den Vorstand führt ein Verzeichnis von Verarbeitungstätigkeiten und – soweit die AWG „Eisenach“ eG, vertreten durch den Vorstand als Auftragsverarbeiter tätig ist – auch ein Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter i. S. d. Art. 30 Abs. 2 DS-GVO.

Das Verzeichnis von Verarbeitungstätigkeiten wird vom externen Datenschutzbeauftragten geführt. Er trägt Sorge dafür, dass die Verarbeitungsverzeichnisse regelmäßig aktualisiert werden und stimmt sich dazu eng mit dem Datenschutzkoordinator ab.

Alle Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungstätigkeiten personenbezogener Daten bei der AWG „Eisenach“ eG, vertreten durch den Vorstand oder für eine Verarbeitung selbst als „Eigentümer“ verantwortlich sind, sind bei einer geplanten Einrichtung oder Änderung von Verarbeitungstätigkeiten und/oder Geschäftsprozessen verpflichtet, dieses dem Datenschutzkoordinator mitzuteilen, dies erfolgt schriftlich oder per E-Mail.

Der externe Datenschutzbeauftragte prüft das Verzeichnis der Verarbeitungstätigkeiten regelmäßig und nach Änderungen.

9 Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der AWG „Eisenach“ eG, vertreten durch den Vorstand oder an Empfänger innerhalb der AWG „Eisenach“ eG, vertreten durch den Vorstand unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten entsprechend geltenden Rechts und dieser Richtlinie. Der Empfänger der Daten muss vertraglich darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden – etwa im Rahmen eines Vertrages zur Auftragsverarbeitung i. S. d. Art. 28 DS-GVO oder einer allgemeinen Verpflichtungserklärung zur Vertraulichkeit.

Die Übermittlung personenbezogener Daten an Dritte, gleich in welcher Form (telefonisch, textlich), z. B. bei Auskunftsersuchen von Sozialämtern, gesetzlichen Betreuern/Bevollmächtigten und (Strafverfolgungs-) Behörden erfordert eine Bewertung im Einzelfall durch den Verantwortlichen und den Datenschutzkoordinator. Der externe Datenschutzbeauftragte sollte im Bedarfsfall unmittelbar eingebunden werden.
Im Falle einer Datenübermittlung von Dritten an die AWG „Eisenach“ eG, vertreten durch den Vorstand muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet und übermittelt werden dürfen. Potentielle Verstöße sind der anderen Seite anzuzeigen und entsprechende interne Maßnahmen zu ergreifen.

10 Datenschutz-Folgenabschätzung

Der Datenschutzkoordinator wird in Zusammenarbeit mit dem externen Datenschutzbeauftragten jede neue, gemeldete Verarbeitungstätigkeit dahingehend prüfen, ob damit voraussichtlich ein hohes Risiko für personenbezogene Daten einhergeht. Gleiches gilt für die Veränderung von Verarbeitungstätigkeiten.

Wenn ein voraussichtlich hohes Risiko besteht, wird der Datenschutzkoordinator der Geschäftsleitung die Durchführung einer Risikoanalyse und in der Folge eine Datenschutz-Folgenabschätzung (DSFA) empfehlen. Die Geschäftsleitung entscheidet über das „Ob“ und „Wie“ der Durchführung der DSFA auf der Grundlage des Ergebnisses der Risikoanalyse.

Die jeweilige Verarbeitung darf grundsätzlich erst nach Durchführung der DSFA und entsprechender Freigabe durch den externen Datenschutzbeauftragten und die Geschäftsleitung begonnen werden.

Die DSFA kann vom Datenschutzkoordinator durchgeführt werden. Die DSFA kann auch durch externe, fachkundige Personen durchgeführt werden. Der externe Datenschutzbeauftragte (DSB) steht bei der Durchführung der DSFA auf Anfrage für die Beratung zur Verfügung.

Das Ergebnis der DSFA wird dem externen Datenschutzbeauftragten und der Geschäftsleitung mitgeteilt. Die Geschäftsleitung und der externe Datenschutzbeauftragte entscheiden über die Freigabe des Verarbeitungsprozesses.

Sollte die DSFA ergeben, dass das mit dem Verarbeitungsprozess verbundene Risiko nicht durch technische und organisatorische Maßnahmen eingedämmt werden kann, wird die Geschäftsleitung in Zusammenarbeit mit dem externen Datenschutzbeauftragten darüber entscheiden, ob eine vorherige Konsultation mit der Aufsichtsbehörde i. S. d. Art. 36 DS-GVO durchzuführen ist.

11 Rechte des Betroffenen

Jeder Betroffene kann Rechte im Zusammenhang mit der Verarbeitung seiner Daten wahrnehmen. Ihre Geltendmachung ist umgehend mit dem externen Datenschutzbeauftragten abzustimmen und durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

Für die Prüfung und Umsetzung der Geltendmachung gelten die folgenden Anforderungen:

- Die Geltendmachung muss innerhalb von 4 Wochen beantwortet werden.
- Kann dies nicht in der festgelegten Frist erfolgen, so muss der Antragsteller über die Gründe und den Termin der Verschiebung informiert werden.
- Der Antragsteller zur Geltendmachung muss vor Umsetzung eindeutig identifiziert werden.

- Der Antrag muss unverzüglich zur Prüfung und Beantwortung an den externen Datenschutzbeauftragten weitergeleitet werden.
- Die Umsetzung der Geltendmachung muss grundsätzlich unentgeltlich erfolgen.
- Wenn Geltendmachungen offenkundig unbegründet sind bzw. in häufiger Wiederholung auftreten, können Maßnahmen des Art. 12 Abs. 5 DS-GVO gegen den Betroffenen ergriffen werden. Dabei hat das Unternehmen den Nachweis für den offenkundig unbegründeten bzw. exzessiven Charakter des Ersuchens zu erbringen.
- Im Falle einer Auftragsverarbeitung, sind die einzelnen Prozessschritte vom Auftragnehmer durchzuführen und zu dokumentieren. Der Auftraggeber hat vor Information an den Betroffenen die Umsetzung und Dokumentation der Löschung bzw. Beschränkung zu prüfen und zu dokumentieren.

Die Ausübung folgender Rechte kann ein Betroffener beantragen:

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind (Art. 15 DS-GVO).
   Falls im Arbeitsverhältnis nach arbeitsrechtlichen Regelungen weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z. B. Personalakte) vorgesehen sind, so bleiben diese unberührt.

   Dabei gelten die folgenden zusätzlichen Anforderungen:

   a) Auskunftsersuchen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Zudem ist das Auskunftsersuchen aus Gründen der Dokumentation schriftlich zu beantworten.
   b) Auskunftsanfragen durch Betroffene werden grundsätzlich durch den externen Datenschutzbeauftragten (DSB) beantwortet.
   c) Eine Beantwortung durch die Beschäftigten ist untersagt.
   d) Die Fachabteilungen unterstützen den externen DSB bei der Beantwortung der Auskunftsanfragen.

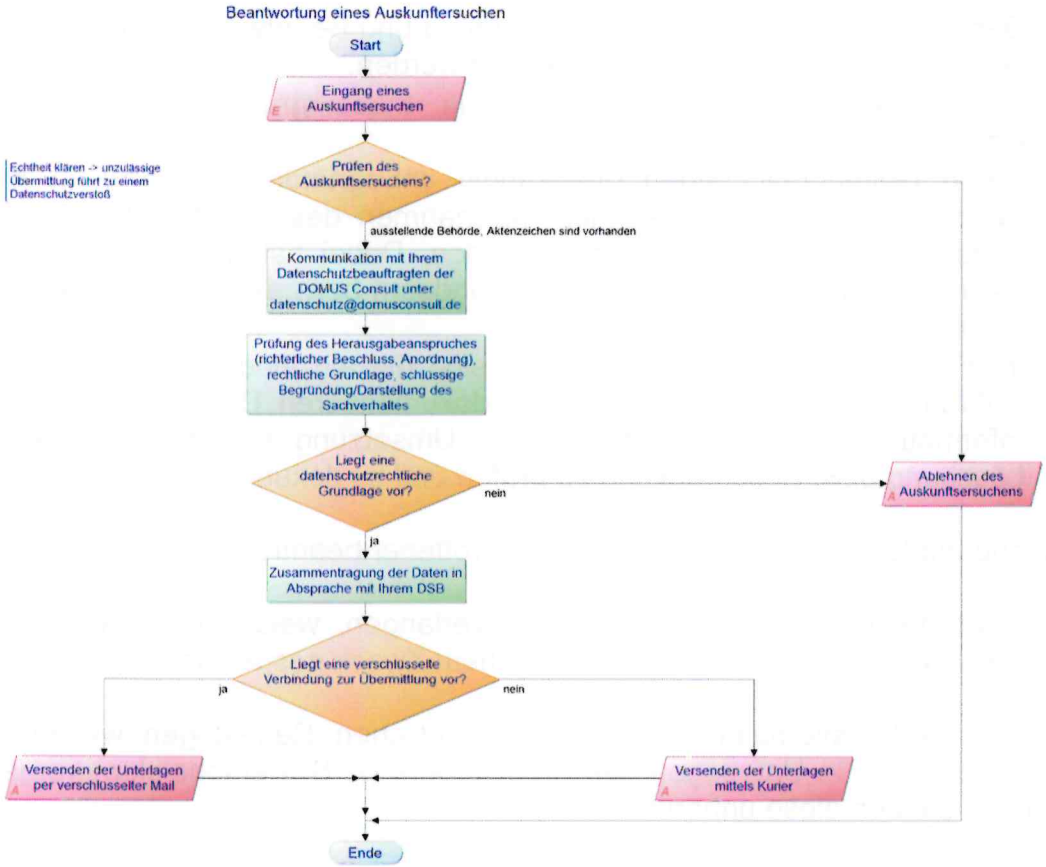

Abbildung 1: Beantwortung eines Auskunftsersuchens

2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden (Art. 15 DS-GVO).
3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
4. Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn:
   a) die Rechtsgrundlage für die Verarbeitung der Daten fehlt, weggefallen ist.
   b) der Betroffene ein überwiegendes schutzwürdiges Interesse am Ausschluss der Verarbeitung nachweisen kann.
   c) der Zweck der Datenverarbeitung durch gesetzliche Frist oder aus anderen Gründen entfallen ist.

   Vor Löschung muss geprüft werden ob eine Aufbewahrungsfrist für die Daten existiert, die einer Löschung entgegensteht. Ist dies der Fall, ist die Einschränkung der Verarbeitung (ggf. durch Sperrung) der Daten durchzuführen.
   Als berechtigt einzustufende Löschersuchen werden durch den Datenschutzkoordinator dokumentiert. Die Datenlöschung kann durch den Datenschutzkoordinator erfolgen. Der externe DSB ist im Bedarfsfall einzubinden. Die Umsetzung ist zwingend zu dokumentieren.

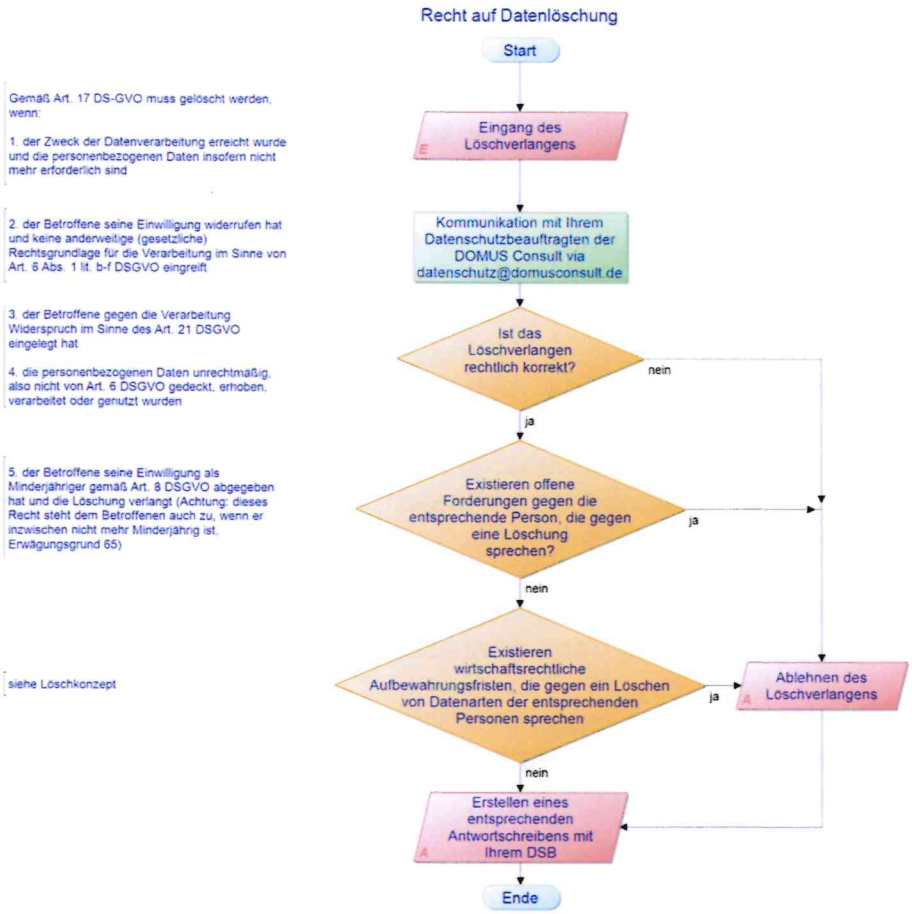

Abbildung 2:Recht auf Datenlöschung

5. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn etwa sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn ein Erlaubnistatbestand zur Durchführung der Verarbeitung vorliegt.
6. Der Betroffene hat ein Recht auf Datenübertragbarkeit seiner personenbezogenen Daten in einem gängigen, maschinenlesbaren Format – soweit dies technisch machbar ist.
7. Der Betroffene hat das Recht, eine in der Vergangenheit erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen.

12 Verarbeitung personenbezogener Daten durch einen Dienstleister

Sollte zur Erfüllung der Aufgaben der Einsatz eines Dienstleisters notwendig sein und im Rahmen der Tätigkeit die Verarbeitung personenbezogener Daten stattfinden, so ist mit dem Dienstleister eine Vertraulichkeitsvereinbarung abzuschließen. Alle Dienstleister sind in der Übersicht der Dienstleister zu ergänzen.

Sollte der Dienstleister die Verarbeitung der personenbezogenen Daten weisungsgebunden für die AWG „Eisenach“ eG, vertreten durch den Vorstand durchführen und die Datenverarbeitung nicht einen bloßen Nebenzweck der

Geschäftstätigkeit des Auftragnehmers umfassen, so ist mit dem Dienstleister eine Vereinbarung über eine

Auftragsverarbeitung abzuschließen. Der Auftragnehmer darf personenbezogene Daten grundsätzlich nur im Rahmen der Weisungen des Auftraggebers verarbeiten und muss eventuell beauftragten Subunternehmern entsprechende Verpflichtungen auferlegen, die zwischen Auftraggeber und Auftragnehmer bestehen. Die Anforderungen ergeben sich im Einzelnen aus Art. 28 der EU-Datenschutz-Grundverordnung (DS-GVO).

Eine Auftragsverarbeitung darf nur mit Auftragnehmern durchgeführt werden, die hinreichende Garantien und Sicherheiten für die im Auftrag zu verarbeitenden Daten erbringen – dies ist zumindest stichprobenartig zu prüfen (etwa durch Nachweise von Zertifikaten, Testaten, IT-/-Datenschutzprüfungen, Berechtigungs-, Notfall- und Löschkonzepte usw.).

Die für den Datenschutz bereitgestellten Vertragsklauseln/technischen organisatorischen Maßnahmen laut Vertrag müssen beachtet werden.

Vor Abschluss einer Vereinbarung muss die Prüfung und Abstimmung der Verträge durch die Geschäftsleitung in Abstimmung mit dem Datenschutzkoordinator und dem externen Datenschutzbeauftragten erfolgen.

13 Umgang mit Vorfällen

Ein Vorfall ist jedes Vorkommnis, bei dem die Schutzziele des Datenschutzes, Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten und die zur Verarbeitung genutzten IT-Systeme, in unzulässiger Weise verletzt werden. Im Falle eines Vorkommnisses ist es wichtig, dass die Beschäftigten und verantwortliche Ansprechpartner nach definierten Verhaltensregeln agieren um eine weitere Beeinträchtigung der Daten und IT-Systeme, durch in der Situation unangemessenes Verhalten zu vermeiden.

13.1 Kategorisierung und Priorisierung von datenschutzrelevanten Vorfällen

Potentieller Datenschutzvorfall

Ein potentieller Datenschutzvorfall ist ein erkanntes Auftreten eines fehlerhaften Zustandes eines IT-Systems, der zu einer Verletzung des Schutzziels Vertraulichkeit führen kann.

Weiterhin sind alle Ereignisse potentielle Datenschutzvorfälle, bei denen eine Beeinträchtigung des Schutzziels „Vertraulichkeit“ stattfinden kann, auch wenn diese Ereignisse nicht im Zusammenhang mit der EDV des Unternehmens stehen.

Datenschutzvorfall

Ein Datenschutzvorfall ist ein einzelner oder eine Reihe von unerwünschten oder unerwarteten potentiellen Datenschutzvorfällen, bei denen eine erhebliche

Wahrscheinlichkeit besteht, dass personenbezogene Daten so kompromittiert werden, dass das angestrebte Sicherheitsniveau bedroht ist.

Eine (vermeintlich) vorsätzlich herbeigeführte Verletzung des Sicherheitsniveaus ist unabhängig von den Auswirkungen auf die Daten immer ein Datenschutzvorfall.

Kritischer Datenschutzvorfall

Ein kritischer Datenschutzvorfall liegt immer dann vor, wenn mit schwerwiegenden Auswirkungen auf die Rechte von Betroffenen zu rechnen ist. Das Sicherheitsniveau personenbezogener Daten ist einem Maße bedroht, dass das Schutzniveau nicht mehr gewährleistet werden kann.

Beispiel für einen kritischen Datenschutzvorfall ist ein unberechtigter Zugriff auf ein IT-System mit einem (vermuteten) Abfluss bzw. Verlust von personenbezogenen Daten.

13.2 Prozess der Vorfallbehandlung

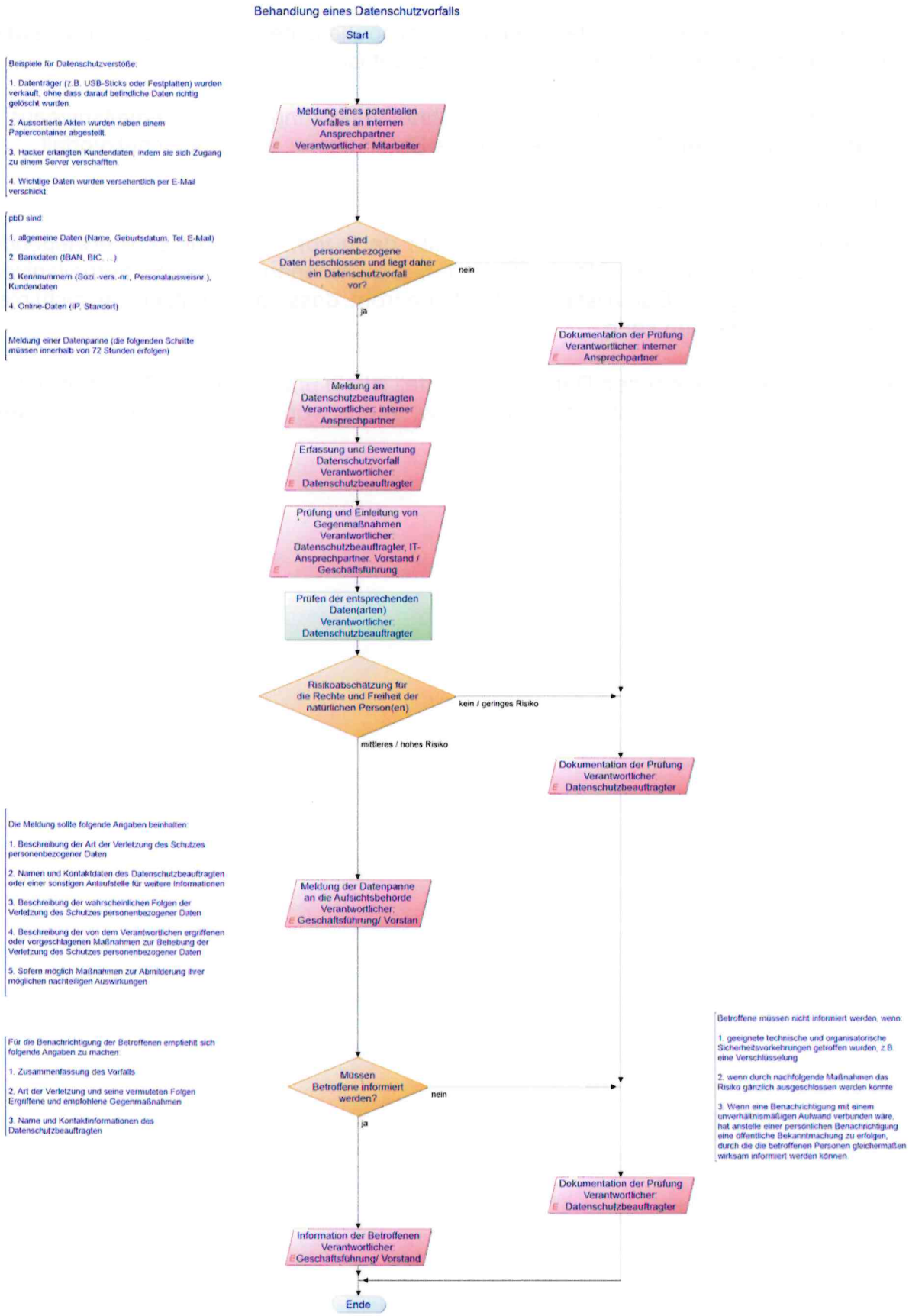

Abbildung 3: Prozess Behandlung eines Datenschutzvorfall

Meldung und Erfassung
Die Meldung eines potentiellen Datenschutzvorfalls kann durch Beschäftigte oder Dienstleister telefonisch oder per E-Mail an den Vorgesetzten bzw. internen Ansprechpartner erfolgen. Der Vorgesetzte bzw. interne Ansprechpartner meldet diesen an den Datenschutzkoordinator. Dieser bewertet und dokumentiert den potentiellen Datenschutzvorfall und bindet den externen DSB ein.

Die Meldung an den externen Datenschutzbeauftragten muss mindestens nachfolgende Angaben enthalten:
- Kontaktdaten der Person, welche den Vorfall meldet,
- Datum/Uhrzeit der Entdeckung,
- kurze Beschreibung des Vorfalls,
- ggf. Unterlagen zur Beweissicherung (Screenshots u. ä.).

Bewertung
Im Prozessschritt Bewertung ist durch den externen DSB zu prüfen, ob es sich tatsächlich um einen Datenschutzvorfall handelt. Ist dies nicht der Fall, ist der Vorgang durch den externen DSB zu dokumentieren und zu archivieren.

Liegt ein Datenschutzvorfall vor, ist das Risiko, welches sich mit dem Vorfall verbindet, zu bewerten. In Abhängigkeit von dem Risiko sind die Meldepflichten an die Aufsichtsbehörde bzw. Betroffene zu prüfen und ggf. umzusetzen.

Der externe DSB priorisiert und kategorisiert den Vorfall. Handelt es sich bei dem Vorfall um einen Notfall, wird dieser durch den externen DSB entsprechend an das Notfallmanagement eskaliert.

Zudem ist durch den externen DSB zu prüfen, ob der Vorfall schon einmal aufgetreten ist und es entsprechende Behandlungsmöglichkeiten gibt („Known-Error“).

Einleitung Sofortmaßnahmen
Sofern der Vorfall als Datenschutzvorfall kategorisiert wurde, ist durch den externen DSB in Abstimmung mit der Leitungsebene die Einleitung von Sofortmaßnahmen zu prüfen, um die Kompromittierung personenbezogener Daten zu verhindern bzw. einzudämmen. Die Sofortmaßnahmen sind durch die IT-Administration bzw. die Fachabteilungen umzusetzen.

Analyse
Zur Ableitung geeigneter Maßnahmen zur Behebung der Folgen des Datenschutzvorfalls und zur Prävention vergleichbarer Vorfälle wird dieser durch den externen DSB unter Einbeziehung des Datenschutzkoordinators und der IT-Administration oder weiterer Fachabteilungen einer weiteren Analyse unterzogen. Dazu werden die genaueren Umstände des Vorfalls betrachtet.

Gegenstand der Analysen sind:
- die genauen Umstände des Vorfalls,
- der Umfang betroffener Systeme, Anwendungen und ihrer Daten sowie ihre Gefährdung,
- mögliche Folgeschäden und Risiken für die Betroffenen,
- bekannte oder vermutete Ursachen,

- eingetretene oder zu erwartende Außenwirkung,
- Maßnahmen zur Behandlung des Vorfalls,
- Maßnahmen zur Prävention vergleichbarer Vorfälle,
- Überlegungen, wann und in welchen Schritten ggf. ergriffene Sofortmaßnahmen (z.B. Systemabschaltung) zurückgenommen werden können.

Einleitung von Gegenmaßnahmen
Die Erarbeitung und Durchführung geeigneter Gegenmaßnahmen erfolgt unter Beteiligung der Leitungsebene, des externen Datenschutzbeauftragten, dem IT-Administrator sowie den jeweiligen fachlich verantwortlichen Abteilungen je nach Bedarf. Sofern der Vorfall bei einem externen Dienstleister aufgetreten ist bzw. dessen Unterstützung zur Behebung des Vorfalls erforderlich ist, ist der Dienstleister entsprechend der vertraglichen Vereinbarung einzubinden. Die Umsetzung der festgelegten Maßnahmen zur Behebung des Vorfalls obliegt den zuständigen Fachbereichen.

Anlassbezogenes Audit und Wiederaufnahme des Geschäftsbetriebs
Bei Auftreten eines Datenschutzvorfalls ist das Sicherheitsniveau des Unternehmens kompromittiert worden. Um festzustellen, ob die Umsetzung der in der Analyse festgelegen Gegenmaßnahmen ausreichend ist, um das angestrebte Sicherheitsniveau wiederherzustellen, ist durch den externen Datenschutzbeauftragten ein anlassbezogenes Audit durchzuführen. Wird im Rahmen des Audits festgestellt, dass das angestrebte Sicherheitsniveau durch die eingeleiteten Maßnahmen nicht wiederhergestellt werden konnte, ist der Vorgang erneut zu analysieren.
Wird im Rahmen des Audits festgestellt, dass das angestrebte Sicherheitsniveau durch die eingeleiteten Maßnahmen wiederhergestellt werden konnte, ist der Vorgang abzuschließen und das System bzw. der Prozess in den regulären Geschäftsbetrieb zu überführen.

Meldepflichten
Die zuständige Aufsichtsbehörde ist gem. Art. 33 DS-GVO bei jeder Verletzung des Schutzes personenbezogener Daten zu informieren. Eine Verletzung des Schutzes personenbezogener Daten bedeutet in diesem Zusammenhang konkret die „Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“. (Art. 4 Absatz 12 DS-GVO)

Die Meldung des Datenschutzvorfalls muss, unabhängig vom Empfänger der Meldung, nachfolgende Informationen beinhalten:

- Art der Verletzung,
- Kontaktdaten des Datenschutzbeauftragten oder eines anderen Ansprechpartners,
- Mögliche Folgen der Datenschutzverletzung,
- Ergriffene Maßnahmen um das Risiko für die Betroffenen zu minimieren.

Die Meldung an die Aufsichtsbehörden muss zudem nachfolgende zusätzliche Informationen enthalten:

- Anzahl der Betroffenen,
- Kompromittierte Datenkategorien,
- Anzahl der kompromittierten Datensätze.

Die Meldung an die Aufsichtsbehörde muss innerhalb von 72 Stunden nach Erkennen des Vorfalls durch die Geschäftsleitung erfolgen.

Die Prüfung der Meldepflichten an den Betroffenen wird durch den externen Datenschutzbeauftragten durchgeführt. Dieser prüft zunächst, ob durch den Vorfall ein Risiko für die Rechte und Freiheiten der Betroffenen entstanden ist. Wenn keine Risiken für die Betroffenen entstanden ist, wird der Vorgang dokumentiert und geschlossen.

Ist das Risiko als hoch zu bewerten, beispielsweise bei der Verletzung von Grundrechten der Betroffenen, sind die Betroffenen unverzüglich gem. Art. 34 DS-GVO von der Datenschutzverletzung „in klarer und einfacher Sprache“ zu unterrichten. Ist der Aufwand unverhältnismäßig, beispielsweise wenn eine sehr hohe Anzahl an Betroffenen informiert werden muss, ist eine öffentliche Bekanntmachung umzusetzen.

Eine Benachrichtigung des Betroffenen oder eine öffentliche Bekanntmachung kann nach Art. 34 Abs. 3 a oder b DS-GVO allerdings unterbleiben, wenn insbesondere durch bereits vor der Datenpanne ergriffene technische und organisatorische Maßnahmen eine unbefugte Kenntnisnahme der Daten durch Dritte ausgeschlossen werden kann.

Eine Benachrichtigung des Betroffenen ist auch dann nicht erforderlich, wenn durch nach der Datenpanne ergriffene Maßnahmen das „hohe Risiko für die Rechte und Freiheiten der betroffenen Personen“ nicht mehr besteht. In diesem Fall bleibt allerdings eine Meldepflicht gegenüber der Aufsichtsbehörde bestehen.

14 Verantwortlichkeiten und Sanktionen

Die Geschäftsleitung der AWG „Eisenach“ eG, vertreten durch den Vorstand sowie alle Beschäftigten sind verantwortlich für die Datenverarbeitung. Sie sind verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden. Durch personelle, organisatorische und technische Maßnahmen ist eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes zu gewährleisten. Bei Datenschutzkontrollen durch Behörden sind der/die Ansprechpartner/in unverzüglich zu informieren.
Der Datenschutzkoordinator ist Bindeglied zwischen Wohnungsunternehmen, Geschäftsleitung und externem Datenschutzbeauftragten.

Der externe Datenschutzbeauftragte kann Kontrollen durchführen und hat die Beschäftigten mit den Inhalten der Datenschutzrichtlinien vertraut zu machen. Die Geschäftsleitung der AWG „Eisenach“ eG, vertreten durch den Vorstand ist verpflichtet, den externen Datenschutzbeauftragten in seiner Tätigkeit zu unterstützen und diesen im Rahmen

gesetzlicher Datenschutzverpflichtungen des Wohnungsunternehmens zu Rate zu ziehen. Die Führungskräfte müssen sicherstellen, dass ihre Beschäftigten im erforderlichen Umfang zum Datenschutz geschult und eingewiesen werden.

Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht können auch strafrechtlich verfolgt werden und Schadensersatzansprüche nach sich ziehen. Datenschutzverstöße sind Gegenstand von **hohen Bußgeldern und anderen Sanktionen durch Gerichte und Aufsichtsbehörden**. Zuwiderhandlungen, für die einzelne Beschäftigte verantwortlich sind, können zu **arbeitsrechtlichen Sanktionen** führen.

Eisenach, den 10.11.2025

Conny Rauschenberg
Vorstand

Johannes Blechinger
Vorstand