Datenschutzrichtlinie
Eigenbetrieb Stadtentwässerung Lingen

Stand: Juli 2020

Inhaltsverzeichnis

§ 1 Bedeutung, Ziel, Zugänglichkeit

(1) Diese Datenschutzrichtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten im Eigenbetrieb Stadtentwässerung Lingen (im Folgenden „Eigenbetrieb" genannt).

(2) Mit dieser Datenschutzrichtlinie sollen die Grundrechte und Grundfreiheiten von Betroffenen, insbesondere ihr Recht auf Schutz personenbezogener Daten gewahrt und geschützt werden.

(3) Die Datenschutzrichtlinie muss für alle Beschäftigten und leitenden Angestellten jederzeit leicht zugänglich sein.

§ 2 Geltungsbereich

(1) Diese Datenschutzrichtlinie findet Geltung für alle von dem Eigenbetrieb verwalteten Geschäftseinheiten.

(2) Sie gilt persönlich für alle Beschäftigten sowie leitenden Angestellten des Eigenbetriebs.

(3) Die Gebote und Verbote dieser Datenschutzrichtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch oder in Papierform vonstatten geht. Ebenso beziehen sie alle Arten von Betroffenen (Kunden, Beschäftigte, Lieferanten etc.) in ihren Geltungsbereich ein.

§ 3 Begriffsbestimmungen

(1) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Kundendaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z.B. beim Autokennzeichen. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

(2) Besondere Arten personenbezogener Daten sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

(3) Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(4) Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

(5) Profiling bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogene Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

(6) Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(7) Verantwortlicher ist 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.

(8) Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(9) Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

(10) Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogene Daten zu verarbeiten.

(11) Eine Einwilligung des Betroffenen ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.

§ 4 Datenschutzorganisation

(1) Der Eigenbetrieb hat den folgenden externen Datenschutzbeauftragten benannt:

Herrn Erden Yücel, FYNE Consulting GmbH, Kaiserstraße 10b - 49809 Lingen, Tel.: 0591 900 26 953, E-Mail.: info@fyne-consulting.com

(2) Der Datenschutzbeauftragte überwacht die Einhaltung der DS-GVO, BDSG sowie anderer gesetzlichen Vorgaben, einschließlich der Vorgaben dieser und anderer Richtlinien des Eigenbetriebs zum Datenschutz. Der Datenschutzbeauftragte berät und unterrichtet die Eigenbetriebsleitung hinsichtlich bestehender Datenschutzpflichten und ist zuständig bei der Kommunikation mit Aufsichtsbehörden. Ausgewählte

Prozesse werden stichprobenartig, risikoorientiert und in angemessenen Zeitabständen durch ihn auf ihre Datenschutzkonformität hin kontrolliert.

(3) Der Datenschutzbeauftragte nimmt seine Aufgaben weisungsfrei und unter Anwendung seines Fachwissens wahr. Er berichtet unmittelbar der Eigenbetriebsleitung.

(4) Der Eigenbetrieb bzw. seine Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen.

§ 5 Umgang mit personenbezogenen Daten

(1) Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach der DS-GVO grundsätzlich verarbeitet werden:

- Bei einem bestehenden Vertragsverhältnis mit dem Betroffenen.

  Beispiel: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen eines Darlehensvertrages.

- Im Zuge vorvertraglicher Maßnahmen auf Anfrage des Betroffenen sowie der Vertragsabwicklung mit dem Betroffenen.

  Beispiel: Kunde K fordert Informationen zu Produkt X an und erwirbt dieses. Die erforderlichen Daten zur Zusendung des Informationsmaterials sowie zur Abwicklung des Rechtsgeschäfts (Lieferung der Ware sowie Zahlung des Kaufpreises) dürfen verarbeitet werden.

- Wenn und soweit der Betroffene eingewilligt hat.

  Beispiel: Der Betroffene meldet sich zum Erhalt eines Newsletters an.

- Wenn eine rechtliche Verpflichtung besteht, der der Eigenbetrieb unterliegt.

  Beispiel: Gesetzliche Aufbewahrungsfristen nach Handelsgesetzbuch (HGB) und Abgabenordnung (AO).

- Wenn berechtigte Interessen des Eigenbetriebs bestehen, sofern nicht die Interessen oder Grundrechte des Betroffenen überwiegen, insbesondere wenn es sich um ein Kind handelt. Datenverarbeitungen unter Berufung auf ein berechtigtes Interesse sollten jedoch nicht ohne vorherige Beratung durch den Datenschutzbeauftragten vorgenommen werden.

  Beispiel: Die Nutzung der postalischen Anschrift zur Aussendung von Werbeschreiben.

(2) Betroffene dürfen nicht einer ausschließlich auf einer automatisierten Verarbeitung - so auch dem Profiling beruhenden Entscheidung unterworfen werden, die ihnen gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(3) Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck, so beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

(4) Falls möglich, sollte auf einen personenbezogene Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen.

(5) Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist - neben der erklärten Einwilligung durch den Betroffenen - nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist. Hierbei sind insbesondere die vernünftigen Erwartungen des Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegenüber des Eigenbetriebs, die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

(6) Der Betroffene ist bei der Erhebung seiner personenbezogenen Daten umfassend über den Umgang mit seinen Daten zu informieren. Die Information hat die Zweckbestimmung, die Identität der verantwortlichen Stelle, die Empfänger seiner personenbezogenen Daten sowie alle sonstigen Information im Sinne des Art. 13 DS-GVO zu beinhalten, um eine faire und transparente Verarbeitung zu gewährleisten. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen.

(7) Werden personenbezogene Daten nicht beim Betroffenen erhoben, sondern werden beispielsweise bei einem anderen Betrieb beschafft, ist der Betroffene nachträglich und umfassend gem. Art. 14 DS-GVO über den Umgang mit seinen Daten zu informieren. Dies gilt auch für die Änderung einer Ziel- und Zweckbestimmung der Datenverarbeitung.

(8) Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die jeweilige Fachabteilung hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

§ 6 Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z.B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

§ 7 Datenübermittlung

(1) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

(2) Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

§ 8 Externe Dienstleister

(1) Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Datenschutzbeauftragte vorab zu informieren.

(2) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- Technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrung des Anbieters im Markt
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.)

(3) Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.

(4) Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

§ 9 Datenminimierung, Privacy by Design/ Privacy by Default

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen („Datenminimierung"). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist. Beispielsweise wird es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den vollen Namen eines Betroffenen zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrunde liegenden Information ebenfalls gewährleisten kann.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern, so insbesondere den Grundsatz der Datenminimierung.

§ 10 Rechte von Betroffenen

(1) Betroffene haben das Recht auf Auskunft über die im Eigenbetrieb über ihre Person gespeicherten personenbezogenen Daten.

(2) Bei der Bearbeitung von Anträgen ist die Identität des Betroffenen zweifelsfrei festzustellen. Bei begründeten Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden.

(3) Die Auskunftserteilung erfolgt schriftlich, es sei denn der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Der Auskunft ist eine Kopie der Daten des Betroffenen beizufügen, die, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie alle weiteren gesetzlich geforderten Informationen nach Art. 15 DS-GVO beinhaltet, um den Betroffenen die Verarbeitung bewusst zu machen und die Rechtmäßigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch des Betroffenen werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Die zuständige IT-Abteilung bzw. der zuständige IT-Ansprechpartner legt den hierfür vorzusehenden Standard fest.

(4) Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.

(5) Der Betroffene hat das Recht auf Löschung seiner personenbezogenen Daten unter den folgenden Voraussetzungen:

- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich.
- der Betroffene hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung - ihre Verarbeitung ist unzulässig,
- der Betroffene legt Widerspruch gegen die Verarbeitung zu Werbezwecken ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen - zu begründenden - persönlichen Situation,
- es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder
- es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

Besteht eine Verpflichtung zur Löschung und wurden die personenbezogenen Daten zuvor öffentlich gemacht, sind weitere Verantwortliche für die Datenverarbeitung über ein Löschbegehren des Betroffenen hinsichtlich aller Kopien seiner Daten sowie aller Links zu diesen Daten zu informieren.

(6) Der Betroffene kann die Einschränkung der Verarbeitung seiner Daten verlangen, wenn

- die Richtigkeit der personenbezogenen Daten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung überprüft wird oder
- die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt, oder
- der Eigenbetrieb die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

- der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.

(7) Der Betroffene ist spätestens innerhalb eines Monats über alle ergriffenen Maßnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.

(8) Der Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

(9) Sämtliche Anfragen und Ersuchen von betroffenen Personen sind an den Datenschutzbeauftragten zu kommunizieren. Der Datenschutzbeauftragte veranlasst alle weiteren notwendigen Maßnahmen zur Erfüllung der Rechte der betroffenen Personen.

§ 11 Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Kunden oder Beschäftigte des Eigenbetriebs, ist eine Weitergabe von Informationen nur zulässig, wenn

- die Auskunft gebende Stelle ein berechtigtes Interesse hierfür darlegen kann, und
- eine gesetzliche Norm zur Auskunft verpflichtet, sowie
- die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

§ 12 Verzeichnis von Verarbeitungstätigkeiten

(1) Der Eigenbetrieb hat ein Verzeichnis über alle Datenverarbeitungen zu führen. Jede Fachabteilung hat eine verantwortliche Person zu benennen, die alle notwendigen Informationen zu den Verfahren der jeweiligen Abteilung nach den gesetzlichen Anforderungen des Art. 30 DS-GVO dokumentiert. Der Datenschutzbeauftragte kann zur Beratung hinsichtlich der gesetzlich geforderten Informationen hinzugezogen werden.

(2) Der Eigenbetrieb stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist der Datenschutzbeauftragte im Einvernehmen mit der Eigenbetriebsleitung.

§ 13 Werbung

(1) Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.

(2) Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig. Bitte konsultieren Sie diesbezüglich den Datenschutzbeauftragten.

§ 14 Schulung

Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Der Datenschutzbeauftragte entscheidet über Form und Turnus der entsprechenden Schulungen.

§ 15 Datengeheimnis

(1) Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen, Sie sind vor Aufnahme ihrer Tätigkeit auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt durch die Eigenbetriebsleitung unter Verwendung des hierzu vorgesehenen Formulars.

(2) Mitarbeiter mit besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis nach § 88 TKG) werden von der Eigenbetriebsleitung ergänzend darauf schriftlich verpflichtet.

§ 16 Beschwerden

(1) Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Datenschutzrichtlinie jederzeit anzeigen.

(2) Die zuständige Stelle für die oben genannten Beschwerden ist der Datenschutzbeauftragte als interne unabhängige und weisungsfreie Instanz.

§ 17 Audits

(1) Um ein hohes Datenschutzniveau zu gewährleisten, werden relevante Prozesse durch regelmäßige Audits interner Stellen oder durch externe Auditoren überprüft. Im Falle einer Feststellung eines Verbesserungspotentials sind unmittelbare Abhilfemaßnahmen zu treffen.

(2) Die beim Audit gewonnenen Erkenntnisse sind zu dokumentieren. Die Dokumentation ist dem Datenschutzbeauftragten, der Eigenbetriebsleitung sowie den Fachverantwortlichen für den jeweiligen Prozess zu übergeben.

(3) Ein Audit ist erfolgreich abgeschlossen, wenn alle im Bericht dokumentierten Maßnahmen umgesetzt sind. Bei Bedarf werden Follow-Up-Audios durchgeführt, indem Empfehlungen des initialen Audits einer Überprüfung ihrer Implementierung unterzogen werden.

§ 18 Interne Ermittlungen

(1) Maßnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen des Betroffenen verhältnismäßig sein.

(2) Der Betroffene ist so bald wie möglich über die zu seiner Person durchgeführten Maßnahmen zu informieren.

(3) Bei allen Formen der internen Ermittlungen ist der Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Maßnahmen vorab einzubeziehen.

§ 19 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) In Abhängigkeit der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Analyse hinsichtlich der Risiken für Betroffene zu erfolgen.

(2) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren verbindlich ist. Hierin ist insbesondere der Stand der Technik ebenso zu berücksichtigen, wie Mittel und Maßnahmen zur Verschlüsselung und Datensicherung. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen, bewerten und zu evaluieren.

(3) Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Türen unbesetzter Räume sind zu verschließen. Wirksame Maßnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit zu sperren.

(4) Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden. Passwörter müssen eine minimale Länge von acht Zeichen aufweisen und aus einem Zeichenmix bestehen. Passwörter dürfen nicht in einem Wörterbuch vorkommen oder aus leicht zu erratenden Begriffen gebildet werden, insbesondere nicht Begriffe, die im Zusammenhang mit dem Eigenbetrieb stehen.

(5) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-To-Know-Prinzip“). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

(6) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

(7) Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

(8) Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

§ 20 Datenschutz - Folgenabschätzung

(1) Jede Fachabteilung ist zur Durchführung von Datenschutz-Folgenabschätzungen für Verfahren, die unter ihrer Verantwortung erfolgen, verpflichtet, wenn ein hohes Risiko für Rechte und Freiheiten von Betroffen aufgrund der Datenverarbeitung zu erwarten ist. Die Datenschutz-Folgenabschätzung enthält alle gesetzlich geforderten Beschreibungen des Art. 35 Abs. 7 DS-GVO.

(2) Der Datenschutzbeauftragte berät die Fachabteilungen bei der Durchführung der Datenschutz-Folgenabschätzung sowie bezüglich der Frage, wann Verarbeitungen ein hohes Risiko für Betroffene beinhalten können.

§ 21 Verletzungen des Schutzes von Daten („Datenpanne")

(1) Sollten Eigenbetriebsdaten unrechtmäßig Dritten offenbart worden sein, ist darüber unverzüglich der Datenschutzbeauftragte zu informieren.

(2) Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

(3) Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt ausschließlich durch den Datenschutzbeauftragten. Betroffene werden durch die Eigenbetriebsleitung informiert, wobei der Datenschutzbeauftragte beratend hinzugezogen wird.

§ 22 Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

§ 23 Rechenschaftspflicht

Die Einhaltung der Vorgaben dieser Richtlinie muss jederzeit nachgewiesen werden können. Hierbei ist insbesondere auf die Nachvollziehbarkeit und Transparenz getroffener Maßnahmen zu achten, so beispielsweise über zugehörige Dokumentationen.

§ 24 Aktualisierung der Richtlinie; Nachweisbarkeit

(1) Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

(2) Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

Ort, Datum	Unterschrift der Eigenbetriebsleitung

Anhang: Passwortrichtlinie

Geltungsbereich

Diese Richtlinie regelt die Gestaltung und Handhabung von Passwörtern, die zur Authentifizierung berechtigter Benutzer eingesetzt werden.

Sie ist im Rahmen der technischen Möglichkeiten für alle Softwareanwendungen anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen.

Geheimhaltung

Passwörter sind geheim zu halten. Sie sind verdeckt einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt oder unverschlüsselt auf Rechnern gespeichert werden. Passwörter sollten, wenn möglich, nicht aufgeschrieben werden. Sie dürfen keinesfalls auf handgeschriebenen Zetteln im Zuordnungsbereich hinterlegt werden.

Länge von Passwörtern

Die Länge der Passwörter richtet sich nach dem Schutzbedarf der Daten und Ressourcen. Sie beträgt mindestens 8 Stellen, da sie den Zugriff auf sensible Daten, insbesondere Gesundheitsdaten ermöglichen.

Komplexität von Passwörtern

Passwörter sollen technisch so komplex wie möglich zusammengesetzt sein (große und kleine Buchstaben, Ziffern, Sonderzeichen). Dies ist der wesentlichste Schutz vor systematischem Ausspähen.

Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Zu vermeiden sind insbesondere:

- Zeichenwiederholungen
- Zahlen und Daten aus dem Lebensbereich des Benutzers
- Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen,
- einfache Ziffern- und Buchstabenkombinationen,
- Zeichen die durch nebeneinanderliegende Tasten eingegeben werden,
- Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen (Trivialpasswörter)

Änderung von Passwörtern

Passwörter sind unverzüglich zu wechseln, wenn der Verdacht besteht, dass sie Dritten bekannt geworden sein könnten. Einstiegs- und Übergangspasswörter sind unverzüglich durch eigene Passwörter zu ersetzen.

Anhang: Nutzung des Faxgerätes

Senden Sie personenbezogene Daten nur dann per Fax, wenn eine schnelle Übermittlung erforderlich ist. Sorgen Sie, wenn möglich, für eine Anonymisierung der Daten (etwa durch Schwärzen des Namens).

Zugriff Unbefugter verhindern

Stellen Sie das Faxgerät so auf, dass Unbefugte weder auf das Gerät selbst noch auf ein- oder ausgehende Telefaxe Zugriff nehmen können.

Vertraulichkeit Empfänger prüfen

Stellen Sie sicher, dass auch auf der Empfängerseite die Vertraulichkeit der Daten gewährleistet ist. Können Sie absehen, wer Ihr Telefax entgegennimmt und welche Sicherheitsvorkehrungen dort gegeben sind?

Faxnummer prüfen

Überprüfen Sie vor der Faxsendung, ob die Telefaxnummer des Empfängers noch aktuell ist.

Richtigen Empfänger prüfen

Prüfen Sie während des Sendevorgangs, ob die im Display angegebene Empfängerkennung mit der von Ihnen gewählten übereinstimmt. Brechen Sie ansonsten die Übermittlung sofort ab. Im Zweifelsfall: Netzstecker ziehen!

Übermittlung sensibler Daten abstimmen

Wenn Sie besonders sensible personenbezogene Daten übermitteln: Vereinbaren Sie sich vorher mit dem Empfänger einen bestimmten Zeitpunkt der Telefax-Übermittlung.

Dokumente entfernen

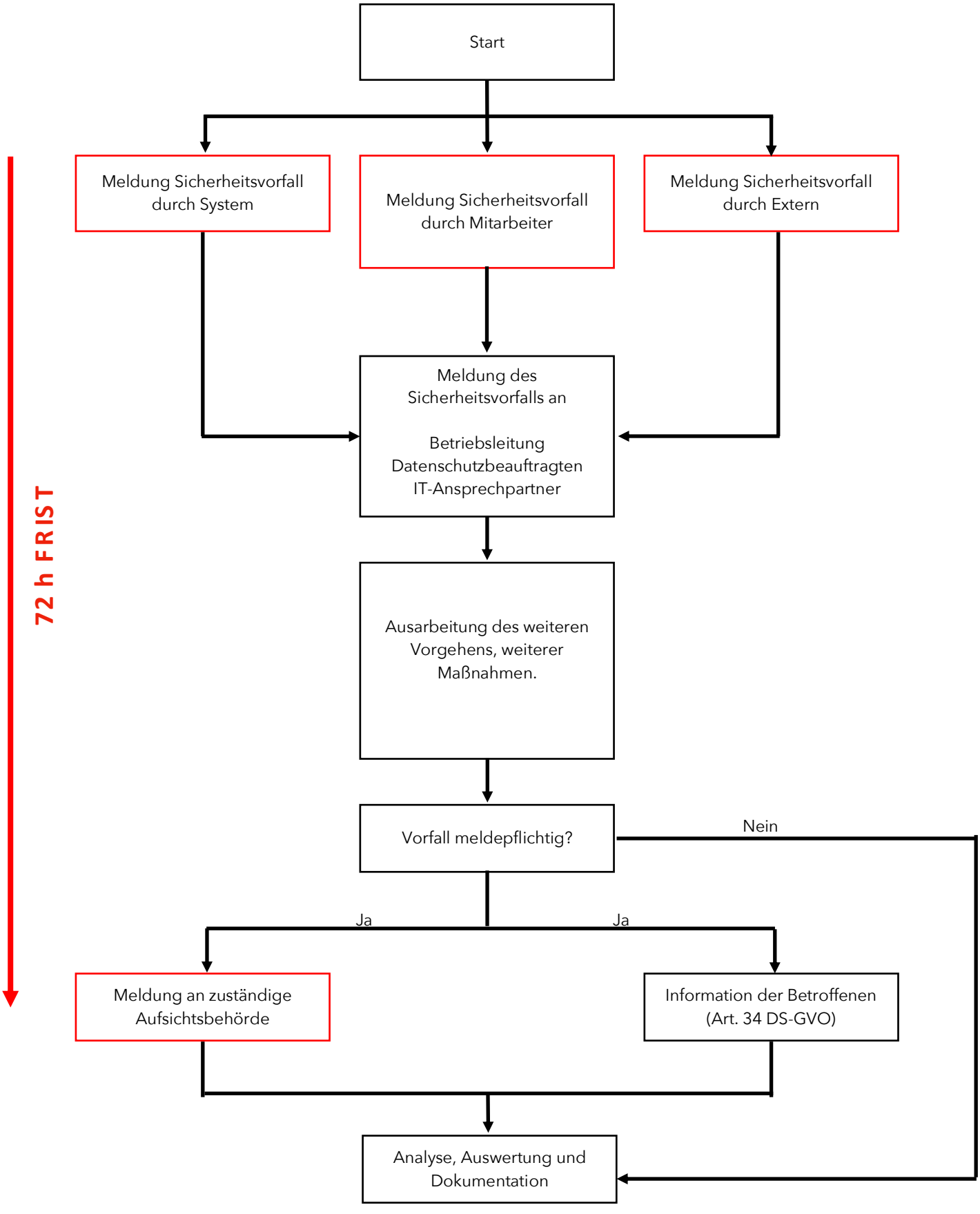
Vergessen Sie keinesfalls, nach erfolgter Sendung die Telefax-Vorlage wieder dem Gerät zu entnehmen.

Sendejournal archivieren

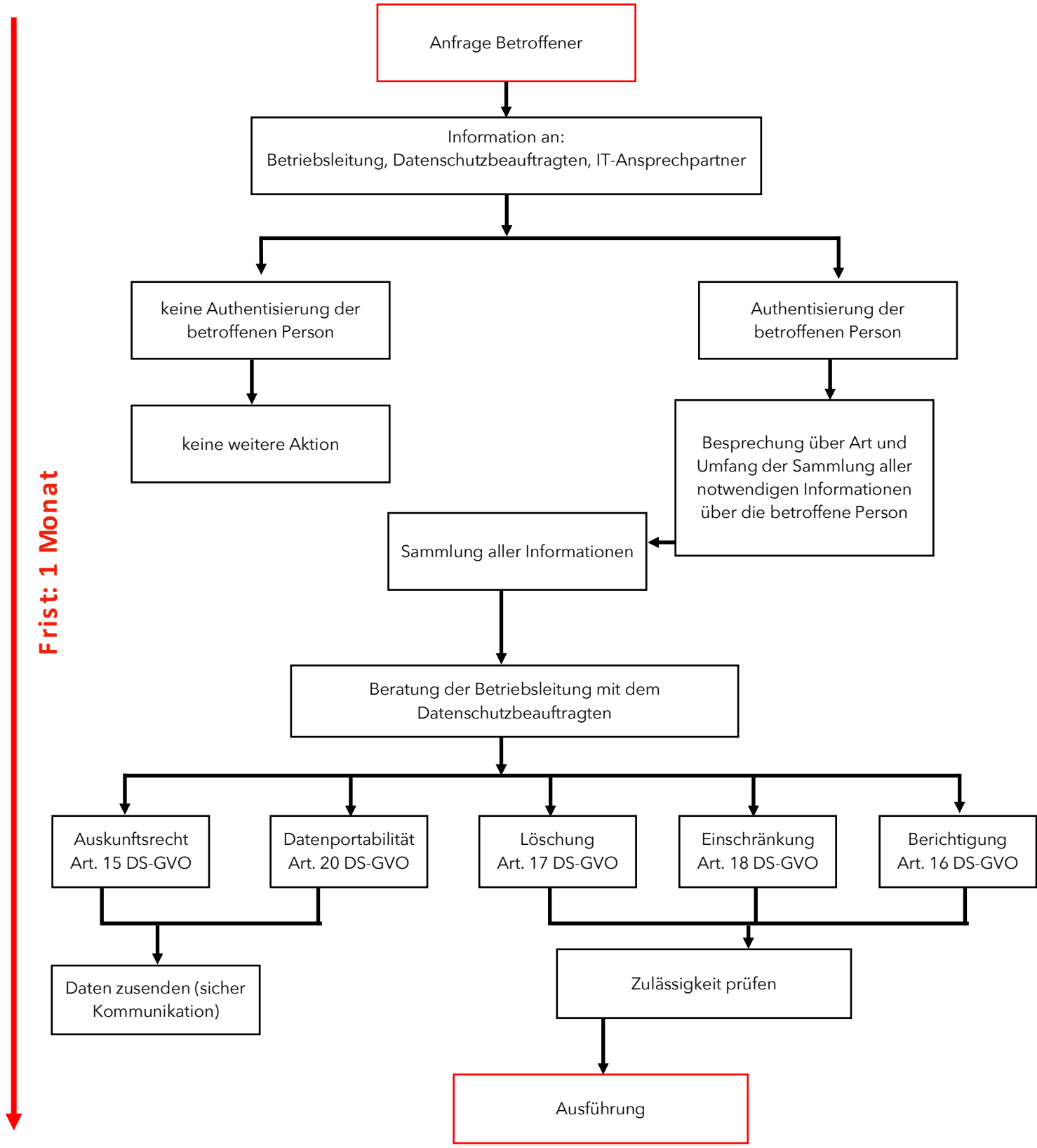
Drucken Sie sich regelmäßig ein Sendejournal aus und archivieren Sie dieses zwei Jahre. Drucken Sie sich bei besonders wichtigen Telefax Dokumenten eine Quittung aus und heften Sie diese an das versandte Original.

Diese Hinweise gelten gleichermaßen für Telefax-Dokumente mit Betriebs- und Geschäftsgeheimnissen. Bitte denken Sie stets daran: Sie sind als Nutzer des Telefaxgeräts für den vertraulichen Umgang mit personenbezogenen Daten verantwortlich.

Anhang: Meldung Sicherheitsvorfall



Anhang: Wahrnehmung Betroffenenrechte



Anlage: Richtlinie Home Office/Mobile Office (Telearbeit)

Gegenstand der Richtlinie, Allgemeines

Diese Richtlinie regelt Fragen des Datenschutzes und der Datensicherheit, wenn Mitarbeitern ein Arbeitsplatz in der eigenen Wohnung oder ein mobiler Arbeitsplatz (Home-Office / Mobile Office - folgend zusammenfassend „Heimarbeitsplatz") durch den Eigenbetrieb Stadtentwässerung Lingen zur Verfügung gestellt wird. Sie ergänzt die allgemeinen betrieblichen Bestimmungen zum Datenschutz und Datensicherheit, die auch am Heimarbeitsplatz stets einzuhalten sind. Im Fall von Widersprüchen geht diese Richtlinie vor.

Ein Heimarbeitsplatz darf nur zur Verfügung gestellt und genutzt werden, wenn die dort zu leistende Tätigkeit zur Erledigung außerhalb des Betriebs geeignet ist, insbesondere mit Blick auf Datenschutz- und Datensicherheitsaspekte. In jedem Fall ist eine schriftliche Vereinbarung mit dem betroffenen Mitarbeiter erforderlich.

Ein Heimarbeitsplatz darf nur zur Verfügung gestellt und genutzt werden, wenn der Mitarbeiter eine Schulung über Datenschutz und Datensicherheit bei Nutzung von Heimarbeitsplätzen absolviert hat, die in angemessenen Abständen zu wiederholen ist. Ist eine solche Schulung ausnahmsweise nicht erforderlich, darf ein Heimarbeitsplatz auch mit Zustimmung der Betriebsleitung zur Verfügung gestellt und genutzt werden.

Umgang mit Daten

Auch wenn Mitarbeiter an ihrem Heimarbeitsplatz tätig werden, bleiben sie Teil von unserem Betrieb. Dies bedeutet, dass alle vertraglichen Weisungsrechte bestehen bleiben und insbesondere alle betrieblichen Daten, Informationen und Unterlagen, auf die Mitarbeiter von ihrem Heimarbeitsplatz aus Zugriff haben, ausschließlich in unserem Hoheitsbereich bleiben. Allen Mitarbeitern ist es daher untersagt, betriebliche Daten, Informationen oder Unterlagen - insbesondere personenbezogene und sonst vertrauliche Daten - an Dritte weiterzugeben, sie Dritten zur Kenntnis gelangen zu lassen (etwa durch Einsichtnahme am Bildschirm oder auf Ausdrucken), sie auf eigenen Speichermedien abzuspeichern, unbefugt zu kopieren oder zu anderen als betrieblichen Zwecken zu verwenden.

Insbesondere

- ist es verboten, Dritten Passwörter oder sonstige Zugangsmöglichkeiten zur dienstlichen EDV (z.B. Chipkarten) mitzuteilen oder zugänglich zu machen, z.B.: durch Notieren von Passwörtern oder Lagerung der Chipkarte am Lesegerät;

- ist es verboten, Dritten (z.B. Familienmitgliedern, sonstigen Mitbewohnern, Besuchern) Zugriff auf die betriebliche EDV und/oder betriebliche Unterlagen zu gewähren;

- ist es verboten, betriebliche Daten auf anderen Speichermedien als von uns schriftlich zugelassen zu speichern; zugelassen ist die Speicherung auf betrieblichen Servern (Laufwerk, ...). Verboten ist somit insbesondere die Speicherung von betrieblichen Daten auf privaten Smartphones, USB-Sticks, Computern o.ä.;

- ist es verboten, dienstliche Daten mit privaten Geräten zu verarbeiten; dazu gehört auch der Abruf des dienstlichen E-Mail-Accounts mit einem privaten Computer, Smartphone o.ä.;

- ist es verboten, Sicherheitsmaßnahmen zu deaktivieren oder zu umgehender sonstige technische Veränderungen an den durch uns zur Verfügung gestellten Geräten vorzunehmen. Software darf nur durch eine hierfür gesondert beauftragte Person installiert werden;

- müssen eventuelle Ausdrucke mit vertraulichen Informationen z.B: personenbezogenen Daten) sicher vernichtet werden (z.B. Aktenvernichter, externen Aktenvernichtungsunternehmen)

Alle Störungen oder Auffälligkeiten bei der EDV-Nutzung sind unverzüglich der Betriebsleitung und dem IT-Ansprechpartner zu melden.

Die private Nutzung der für den Heimarbeitsplatz bereitgestellten betrieblichen Geräte bzw. Zugangsmöglichkeiten (insbesondere Computer und Internetzugang) ist verboten.

Wir sind jederzeit berechtigt, vom Mitarbeiter die Herausgabe sämtlicher betrieblicher Daten, Unterlagen und Akten einschließlich sämtlicher Kopien zu verlangen; sind zum Zugriff auf betriebliche Daten Passwörter oder sonstige Schlüssel erforderlich, sind diese mit herauszugeben. Der Mitarbeiter kann hiergegen kein Zurückbehaltungsrecht geltend machen.

Sicherheitsmaßnahmen im Home-Office

Als Heimarbeitsplatz in der Wohnung des Mitarbeiters darf nur ein Raum genutzt werden, der abschließbar ist. Er soll bei Nichtnutzung durch den Mitarbeiter abgeschlossen werden. Hat der Mitarbeiter Gäste (auch Handwerker) in seiner Wohnung, muss der Raum verschlossen sein. Halten sich Dritte am Heimarbeitsplatz auf (z.B. Handwerker, die hier arbeiten müssen), muss der Mitarbeiter sie jederzeit beobachten.

Verlässt der Mitarbeiter seinen Heimarbeitsplatz (und sei es nur kurz, etwa zur Toilette), muss sichergestellt sein, dass kein Dritter auf betriebliche Daten oder Akten zugreifen kann. Dies bedeutet insbesondere, dass

- der verwendete Computer gesperrt werden muss, so dass bei Rückkehr zumindest die Eingabe des Passwortes erforderlich ist;

- Fenster verschlossen sein müssen, außer bei kurzzeitiger Abwesenheit, während der ein Eindringen realistischerweise ausgeschlossen werden kann (z.B. 10. Stock und keine Möglichkeit, aus der Nachbarwohnung herüberzuklettern);

- bei Nutzung von Papier-Akten diese in einem Schrank einzuschließen sind oder der Heimarbeitsplatz-Raum abzuschließen ist; dies gilt nur dann nicht, wenn der Mitarbeiter alleine zu Hause ist und seinen Heimarbeitsplatz nur kurzzeitig verlässt;

- bei Verlassen der Wohnung ein gegebenenfalls genutztes Zugangsmedium (z.B. Chipkarte, Transponder) vom Computer entfernt werden muss und bei Nutzung von Papier-Akten diese in einem Schrank einzuschließen sind.

Zusätzliche Sicherheitsmaßnahmen im Mobile Office

Bei der Nutzung eines mobilen Arbeitsplatzes (Mobile Office) außerhalb der Wohnung des Mitarbeiters gilt ergänzend zu den Regelungen des vorherigen Absatzes:

- Der Mitarbeiter darf den mobilen Arbeitsplatz außerhalb eines verschlossenen Raums nicht - auch nicht kurzzeitig - unbeaufsichtigt lassen, wenn nicht eine Aufsicht durch einen anderen Mitarbeiter aus unserem Betrieb sichergestellt ist. Ausnahmsweise kann der Vorgesetzte Ausnahmen zulassen, wenn der mobile Arbeitsplatz an feste oder ausreichend große Gegenstände angeschlossen, eine ausreichende soziale Kontrolle sichergestellt, die Abwesenheit nur kurz ist und keine besonders vertraulichen Daten verarbeitet werden.

- Bevor der Mitarbeiter seine direkte Aufmerksamkeit vom mobilen Arbeitsplatz entfernt, ist der Computer zu sperren und sind alle Zugangsmedien (z.B. Chipkarte, Transponder) zu entfernen und sicher zu verwahren.

- Die mobile Nutzung von Akten bedarf der vorherigen (schriftlichen) Zustimmung des Vorgesetzten.

- Die Mitnahme des mobilen Arbeitsplatzes ins Ausland bedarf der Zustimmung des Vorgesetzten.

Sicherheitsmaßnahmen beim Transport und bei der Übertragung von Akten und Daten

Jede Mitnahme betrieblicher Daten und Akten benötigt die vorherige schriftliche Zustimmung des Vorgesetzten.

Nimmt der Mitarbeiter betriebliche Akten mit, dürfen diese nur in verschlossenen Behältnissen transportiert werden (z.B. verschlossene Kiste, verschlossener Aktenkoffer). Der Mitarbeiter darf die Akten beim Transport zu keiner Zeit unbeaufsichtigt lassen. Dies gilt auch, wenn das verschlossene Behältnis im Kofferraum eines Autos transportiert wird (z.B. ist ein Verlassen des Fahrzeugs zum Einkaufen auf dem Heimweg nicht zulässig).

Nimmt der Mitarbeiter betriebliche Daten mit, muss der Datenträger mit einem von der Betriebsleitungung freigegebenen Verfahren nach dem Stand der Technik verschlüsselt sein.

Jede Datenübertragung zwischen dem Heimarbeitsplatz und dem Betrieb - einschließlich Terminal-Zugriff - muss nach dem Stand der Technik verschlüsselt sein.

Zugriffe und Zugriffsversuche vom Heimarbeitsplatz werden von uns protokolliert und regelmäßig ausgewertet. Diese Daten werden nur zur Missbrauchsentdeckung, -bekämpfung und -Verfolgung verwendet und nicht zur Leistungs- oder Verhaltenskontrolle.

Kontroll- und Zutrittsrechte zur Wohnung

Der Mitarbeiter räumt folgenden Personen das Recht ein, zur Kontrolle des Heimarbeitsplatzes seine Wohnung zu betreten:

- zur Kontrolle der Daten- und Arbeitssicherheit einer von unserem Betrieb hierfür gesondert beauftragten Person;

- zur Einrichtung, Wartung, Reparatur, Änderung, Abholung der von uns bereitgestellten Arbeitsmittel hierfür gesondert beauftragten Personen;

- zu den gesetzlich vorgesehenen Kontrollen allen Behörden, die den Heimarbeitsplatz aufsuchen dürften, wenn sich dieser im Betrieb befände, beispielsweise der Datenschutz-Aufsichtsbehörde;

- dem Betriebsleiterer, wenn er eine der oben genannten Personen begleitet. Das Zutrittsrecht ist auf den Heimarbeitsplatz (einschließlich zugehöriger Einrichtungen, etwa Telefonanschluss im Keller o.ä.) begrenzt und auf das unbedingt Erforderliche zu beschränken. Jeder Zutritt ist rechtzeitig im Voraus abzustimmen, wobei auf die Interessen des Mitarbeiters, wie beispielsweise Kinderbetreuung, Rücksicht zu nehmen ist, und auf Werktage zu den betrieblich üblichen Geschäftszeiten zu beschränken, es sei denn, aus besonderen Gründen ist ein sofortiger oder kurzfristiger Zutritt oder ein Zutritt zu einem bestimmten Termin unbedingt erforderlich. Im Fall des Zutrittsrechts durch Behörden richten sich eventuelle Abstimmungspflichten und Zeiten nach den Befugnissen der Behörde, die diese hätte, wenn sich der Heimarbeitsplatz im Betrieb befinden würde, und beschränken sich die Pflichten von unserem Betrieb darauf, den Mitarbeiter unverzüglich zu informieren, sobald ihm der

Zutrittswunsch bekannt wird, und auf Wunsch des Mitarbeiters zur Behörde zu vermitteln, um einen anderen Termin zu vereinbaren.

Die Erlaubnis zur Einrichtung und Nutzung des Heimarbeitsplatzes steht zu dem unter der aufschiebenden Bedingung, dass (der Heimarbeitsplatz kann also erst eingerichtet werden, wenn) sämtliche Mitbewohner des Mitarbeiters die gleichen Zutrittsrechte einräumen. Wir können jederzeit verlangen, dass der Mitarbeiter die Zustimmung aller Mitbewohner schriftlich nachweist.

Widerruft der Mitarbeiter oder einer seiner Mitbewohner das Zutrittsrecht oder kommt ein neuer Mitbewohner hinzu, der nicht die Zutrittsrechte nach Abs. 1 einräumt, erlischt automatisch die Berechtigung des Mitarbeiters, den Heimarbeitsplatz zu nutzen. Der Mitarbeiter ist verpflichtet, dies sofort uns gegenüber anzuzeigen, sämtliche betrieblichen Akten und Datenträger sofort in den Betrieb zurückzubringen und seine Arbeitsleistung auf unseren Wunsch hin im Betrieb zu erbringen.

Widerruft der Mitarbeiter oder einer seiner Mitbewohner das Zutrittsrecht oder kommt ein neuer Mitbewohner hinzu, der nicht die gleichen Zutrittsrechte einräumt, können wir zudem verlangen, dass der Mitarbeiter unverzüglich sämtliche von uns bereitgestellten Arbeitsmittel auf eigene Kosten in den Betrieb zurückbringt.

Beendigung der Heimarbeitsplatz-Nutzung

Enden die Berechtigung des Mitarbeiters zur Nutzung des Heimarbeitsplatzes oder das Arbeitsverhältnis oder wird der Mitarbeiter unwiderruflich von der Pflicht zur Arbeitsleistung freigestellt, hat der Mitarbeiter unaufgefordert unverzüglich sämtliche betrieblichen Zugangsmedien (z.B. Chipkarten, Transponder), Datenträger und Akten (einschließlich Kopien) in den Betrieb zurückzubringen und dem Vorgesetzten zu übergeben. Sind zum Zugriff auf betriebliche Daten Passwörter oder sonstige Schlüssel erforderlich, sind diese mit zu übergeben.

Der Mitarbeiter hat zudem die Abholung sämtlicher bereitgestellter Arbeitsmittel durch von uns beauftragte Personen nach angemessener Ankündigungsfrist zu dulden.

Hinweis auf rechtliche Folgen bei Verstößen

Wir weisen darauf hin, dass Verstöße gegen diese Richtlinie nicht nur arbeitsrechtliche Folgen (Ermahnung, Abmahnung, fristgerechte oder fristlose Kündigung) haben, sondern auch mit Geldbuße bedroht und/oder strafbar sein können (z.B. im Fall des Kopierens von Daten nach Art. 83 DS-GVO, § 42 BDSG (gegebenenfalls: § 203 StGB)). Darüber hinaus können Verstöße gegen diese Richtlinie Unterlassungs- und Schadensersatzansprüche nach sich ziehen.

Anlage: Löschkonzept

Scope des beabsichtigten Löschkonzeptes

Bei einem neuen Projekt zur Erstellung eines Löschkonzeptes oder bei der Evaluation bestehender Löschprozesse sollte zunächst wohl überlegt sein, in welchem Umfang und in welcher Detailtiefe die Betrachtung erfolgen soll. Hierbei ist das Ziel einer vollständigen Compliance und das praxisnahe Gebot eines risikoorientierten Ansatzes miteinander abzuwägen.

Abwägung von Lösch- und Aufbewahrungsinteressen

Eine Übersicht über die allgemeinen Aufbewahrungspflichten ist auf der letzten Seite abgedruckt. Jedoch greift mit dem Ablauf der Aufbewahrungsfrist nicht automatisch eine Löschpflicht, da weiterhin ein berechtigtes Interesse an der Archivierung bestehen kann, um z.B. bei Rechtsstreitigkeiten auskunftsfähig zu sein. Umgekehrt kann bei Massendaten von Endkunden teilweise schon vor Ablauf der gesetzlichen Aufbewahrungsfrist eine weitgehende Pseudonymisierung oder gar Anonymisierung durchgeführt werden.

Die Entscheidung, welche Daten nach welcher Frist gelöscht werden sollten, ist daher keine rein rechtliche Frage. Sie sollte daher unter Einbeziehung der Betriebsleitung getroffen werden. Die Verantwortung für das Ergebnis ist aber letztlich vom Verarbeiter zu tragen (u.a. Accountability nach Art. 5 Abs. 2 DS-GVO).

Das frühere Sperren von Daten hat unter der DS-GVO als „Einschränkung der Verarbeitung" (Art. 4 Nr. 3 DS-GVO) für Daten aus Backups und für Daten, die gesetzlichen Aufbewahrungspflichten unterliegen, keine große Relevanz bzw. führt zu keiner besonderen Privilegierung. Insofern ist es außer den in Art. 18 Abs. 1 DS-GVO genannten „Antragssachverhalten" bei neuen Löschkonzepten von keiner großen Bedeutung; jedoch ist bei der Validierung bestehender Löschkonzepte und generell bei der Vorbereitung auf die DS-GVO darauf zu achten, dass die neuen Regeln beachtet werden.

Definition von Datenkategorien und ihren Aufbewahrungsfristen

Für den nach Absatz 1 (Scope des beabsichtigten Löschkonzeptes) festgelegten Scope sind basierend auf dem Abwägungsergebnis aus Absatz 2 nun Datenkategorien zu bilden, denen jeweils konkrete Fristen für die Löschung und/oder für die Einschränkung der Verarbeitung i.S.d. Art. 4 Nr. 3 DS-GVO zugeordnet werden. Hierfür muss in der Regel bekannt sein, zu welchem Zweck die Daten gespeichert und anderweitig verarbeitet werden.

Definition der für die Löschung Verantwortlichen

Nach der Festlegung der Lösch- und Sperrfristen muss konkret festgelegt werden, wer die jeweilige Löschung bzw. die Einschränkung der Verarbeitung (Art. 4 Nr. 3 DS-GVO) umzusetzen hat. Die Löschung selbst kann manuell oder durch einen IT- gestützten Prozess automatisiert erfolgen.

Einbettung in verwandte Themen

Ein gutes Löschkonzept sollte keine Insellösung darstellen, sondern abgestimmt sein mit oder idealiter eingebettet sein in Themen wie

- den Umgang mit individuellen Löschanträgen durch betroffene Personen nach Art. 17 Abs. 1 DS-GVO, die jenseits der standardisierten ggf. automatisierten Prozesse behandelt werden müssen,

- die Prozesse und Berechtigungen zu den weiteren Rechten der Betroffenen, insbesondere auf Auskunftserteilung, Berichtigung, Vergessenwerden, Einschränkung der Verarbeitung und der Datenportabilität (Art. 15 ff. DS-GVO) sowie der Erteilung von Auskünften an Polizei und Strafverfolgungsbehörden,

- ein Berechtigungskonzept (Rollen- und Rechtekonzept), das regelt, welche Personen Zugriff auf welche Daten haben. Hierzu gehört auch ein funktionsfähiges Identity & Access Management (IAM), durch das z.B. sichergestellt wird, dass ausgeschiedenen Mitarbeitern automatisch Zutritts- und Zugangsrechte entzogen werden und bei Tätigkeits- oder Abteilungswechseln die Berechtigungen entsprechend geändert werden.

- die Einbindung in ein vollständiges Informationssicherheitskonzept, das Berechtigungen und Löschungen auch bezüglich nicht-personenbezogener Informationen regelt,

- rechtliche und technische Aspekte bezüglich der Frage, wann eine „echte" Löschung i.S.d. Art. 4 Nr. 2 DS-GVO erfolgt,

- die Dokumentation der Zwecke, zu denen Daten erhoben, gespeichert oder anderweitig verarbeitet werden, da deren Kenntnis eine elementare Voraussetzung für die Bewertung der Speicherfrist ist.

Standards

Zur Wahrung der Compliance mit den gesetzlichen Löschungspflichten kann auf Branchen- und Prozessstandards zurückgegriffen werden.

Übersicht der allgemeinen Aufbewahrungsfristen

Die folgende Übersicht dient lediglich als allgemeine Orientierung. Es ist daher erforderlich jeden Einzelfall gesondert zu prüfen!

Unterlagen	Aufbewahrungsfrist	Rechtsgrundlage
A		
Aboverwaltung	10 Jahre	§ 147 AO, § 257 HGB
Aboverwaltung (nach Vertragsbeendigung)	3 Jahre	§§ 195, 199 BGB
Abrechnungsunterlagen (insofern Belegfunktion)	10 Jahre	§ 147 AO, § 257 HGB
Abtretungserklärungen, soweit erledigt	6 Jahre	§ 147 AO, § 257 HGB
Änderungsnachweise der EDV- Buchführung	10 Jahre	§ 147 AO, § 257 HGB
Akkreditive	6 Jahre	§ 147 AO, § 257 HGB
Aktenvermerke (insofern Belegfuntkion)	10 Jahre	§ 147 AO, § 257 HGB
Aktenvermerke (keine Belegfunktion)	6 Jahre	§ 147 AO, § 257 HGB
Angebote mit Auftragsfolge	6 Jahre	§ 147 AO, § 257 HGB
Angestelltenversicherung (wenn Buchungsbelege)	10 Jahre	§ 147 AO, § 257 HGB
Anhang zum Jahresabschluss (§ 264 HGB)	10 Jahre	§ 147 AO, § 257 HGB
Anlagenvermögensbücher- und Karteien	10 Jahre	§ 147 AO, § 257 HGB
Anträge auf Arbeitnehmersparzulage	10 Jahre	§ 147 AO, § 257 HGB
Aufzeichnungspflicht Arbeitgeber bezüglich der Arbeitszeit von mehr als 8 Stunden werktägig	2 Jahre	§ 16 Abs. 2 ArbZG
Arbeitsanweisungen sofern GoBD relevant (auch für EDV- Buchführung)	10 Jahre	§ 147 AO, § 257 HGB
Arbeitszeitverwaltung Mindestlohn	10 Jahre	§ 147 AO, § 257 HGB

Aufbewahrungsvorschriften für betriebliche EDV-Dokumentation	10 Jahre	§ 147 AO, § 257 HGB
Ausgangsrechnungen	10 Jahre	§ 147 AO, § 257 HGB
Auskunftsverfahren an Betroffene	1 Jahr	Art. 6 Abs. 1 S. 1 c, 17 DSGVO
Außendienstabrechnungen (wenn Buchungsbeleg)	10 Jahre	§ 147 AO, § 257 HGB
Außendienstabrechnungen (wenn sonstiger Beleg)	6 Jahre	§ 147 AO, § 257 HGB
B		
Bankbelege	10 Jahre	§ 147 AO, § 257 HGB
Bankbürgschaften nach Vertragsende	10 Jahre	§ 147 AO, § 257 HGB
Bedienerhandbücher Rechnerbetrieb	10 Jahre	§ 147 AO, § 257 HGB
Belegformate	10 Jahre	§ 147 AO, § 257 HGB
Beitragsabrechnungen zu Sozialversicherungsträgen, wenn Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Belege, soweit Buchungsfunktion (Offene-Posten-Buchhaltung)	10 Jahre	§ 147 AO, § 257 HGB
Sonstige Beitragsabrechnungen des Arbeitgebers mit Sozialversicherungsträgern	Ablauf des auf die letzte Prüfung folgenden Kalenderjahres	§ 28f Abs. 1 SGB IV
Benutzerhandbücher bei EDV- Buchführung	10 Jahre	§ 147 AO, § 257 HGB
Betriebsabrechnungsbögen mit Belegen als Bewertungsgrundlagen	10 Jahre	§ 147 AO, § 257 HGB
Betriebsabrechnungsbögen mit Belegen als Bewertungsgrundlagen	10 Jahre	§ 147 AO, § 257 HGB
Betriebsprüfungsberichte (steuerliche Außenprüfung)	6 Jahre	§ 147 AO, § 257 HGB
Online-Bewerbungen auf Anzeige	Normalerweise 2 bis 6 Monate nach Absage zulässig ohne Einwilligung (Bewerber müssen gem. Art 13 DSGVO bei Eingang über Dauer werden) informiert	§ 26 BDSG, § 15 Abs. 4 AGG, Art. 13 DSGVO
Bewertungsunterlagen	10 Jahre	§ 147 AO, § 257 HGB
Bewirtungsunterlagen (Formblatt, wenn Buchungsbelege oder steuerlich erforderlich)	10 Jahre	§ 147 AO, § 257 HGB
Bilanzen (auch Eröffnungsbilanz)	10 Jahre	§ 147 AO, § 257 HGB
Blockdiagramme, soweit Verfahrensdokumentation	10 Jahre	§ 147 AO, § 257 HGB
Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
C		
Chat und Messenger Protokolle Mitarbeiter (nach Ausscheiden)	3 Monate	Art. 6 Abs. 1 S. 1 f, 17 DSGVO
Chat und Messenger Dienste Kunden / Interessenten (nach Kontakt)	3 Jahre	§§ 195, 199 BGB
D		
Darlehensunterlagen (nach Vertragsende)	6 Jahre	§ 147 AO, § 257 HGB
Darlehensunterlagen als Buchungsbeleg	10 Jahre	§ 147 AO, § 257 HGB
Dauerauftragsunterlagen (nach Ablauf des Auftrags)	10 Jahre	§ 147 AO, § 257 HGB
Dateien, Beschreibungen der	10 Jahre	§ 147 AO, § 257 HGB
Dateiverzeichnisse	10 Jahre	§ 147 AO, § 257 HGB

Datenbankeinträge zu Einwilligungen	Nach Widerruf der Einwilligung	Art. 6 Abs. 1 S. 1 lit. a und b, 17 DSGVO
Datensätze, Beschreibung und Aufbau der	10 Jahre	§ 147 AO, § 257 HGB
Datensicherungsregeln	10 Jahre	§ 147 AO, § 257 HGB
Datenverarbeitung mit stationären Bürogeräten / Multifunktionsgeräten (Drucken, Scannen, Faxen): Cache	Die Daten werden temporär im RAM des Gerätes gespeichert. Der Cache wird aller 2 Wochen geleert, bei Entsorgung des Gerätes werden alle Daten gelöscht und der Speicher ggf. zerstört.	Art. 6 Abs. 1 S. 1 lit. f, 17 DSGVO
Debitorenliste (soweit Bilanzunterlage)	10 Jahre	§ 147 AO, § 257 HGB
Depotauszüge (soweit nicht Inventare)	10 Jahre	§ 147 AO, § 257 HGB
Dienstpläne	1 Jahr	
E		
Einbindung Inhalte Dritter auf Webseiten	Speicherung gemäß Datenschutzerklärungen der Anbieter oder bis auf Widerruf durch Opt-Out.	Datenschutzerklärungen der Anbieter
Einfuhrunterlagen (Anträge, Genehmigungen, Erklärungen, Lizenzen, Zollunterlagen etc.)	10 Jahre	§ 147 AO, § 257 HGB
Eingabebeschreibungen bei EDV- Buchführung	10 Jahre	§ 147 AO, § 257 HGB
Eingabedatenformate	10 Jahre	§ 147 AO, § 257 HGB
Eingangsrechnungen einschließlich Berichtigungsbelege dazu	10 Jahre	§ 147 AO, § 257 HGB
Einheitswertunterlagen	10 Jahre	§ 147 AO, § 257 HGB
E-Mails (Geschäftsbriefe)	6 Jahre	§ 147 AO, § 257 HGB
E-Mails (Buchungsbelege wie Rechnungen)	10 Jahre	§ 147 AO, § 257 HGB
E-Mails (Mahnungen)	6 Jahre	§ 147 AO, § 257 HGB
E-Mail-Newsletter Daten	sofort nach Widerruf oder berechtigtem Löschantrag durch den Betroffenen.	Art. 6 Abs. 1 S. 1 lit. a, 17 DSGVO
Essensmarkenabrechnungen	10 Jahre	§ 147 AO, § 257 HGB
Exportunterlagen	10 Jahre	§ 147 AO, § 257 HGB
F		
Fahrtkostenerstattungsunterlagen	10 Jahre	§ 147 AO, § 257 HGB
Faxe (Geschäftsbriefe)	6 Jahre	§ 147 AO, § 257 HGB
Faxe (Buchungsbelege)	10 Jahre	§ 147 AO, § 257 HGB
Fehlermeldungen, Fehlerkorrekturanweisung bei EDV-Buchführung, wenn Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Fuhrparkdaten (sofern Belegfunktion)	2 Jahre	§ 6 Abs. 1 Nr. 4 S. 4 EStG, § 4 Abs. 5 Nr. 6 EStG
Frachtbriefe	6 Jahre	§ 147 AO, § 257 HGB
G		
Geburtstagsverzeichnis / Jubiläum (nach Ausscheiden)	1 Jahr	Art. 6 Abs. 1 S. 1 lit. a, 17 DSGVO
Gehaltslisten einschließlich Listen für Sonderzahlungen soweit Buchungsbeleg	10 Jahre	§ 147 AO, § 257 HGB
Geschäftsberichte	10 Jahre	§ 147 AO, § 257 HGB

Geschäftsbriefe (zugegangene und Wiedergabe versandter),	6 Jahre	§ 147 AO, § 257 HGB
Geschäftsbriefe als Buchungsbeleg wie z.B. Rechnungen und Gutschriften	10 Jahre	§ 147 AO, § 257 HGB
Geschenknachweise	10 Jahre	§ 147 AO, § 257 HGB
Gewährleistungsunterlagen	6 Jahre	§ 257 HGB, §§ 438, 634 BGB
Gewinn- und Verlustrechnung (nur Jahreserfolgsrechnungen)	10 Jahre	§ 147 AO, § 257 HGB
Gewinnspieldaten der Teilnehmer (nach Ende)	2 Monate	Art. 6 Abs. 1 S. 1 b, 17 DSGVO
Grundbuchauszüge, wenn Inventurunterlagen	10 Jahre	§ 147 AO, § 257 HGB
Grundstücksverzeichnis (soweit Inventar)	10 Jahre	§ 147 AO, § 257 HGB
Gutschriften im Sinne von "umgekehrten Rechnungen"	10 Jahre	§ 147 AO, § 257 HGB
H		
Handelsbriefe (außer Rechnungen oder Gutschriften)	6 Jahre	§ 147 AO, § 257 HGB
Handelsbücher	10 Jahre	§ 147 AO, § 257 HGB
Handelsregisterauszüge, beglaubigte oder soweit im eigenen Interesse erforderlich	10 Jahre	§ 147 AO, § 257 HGB
Handwerkeraufträge	10 Jahre	§ 147 AO, § 257 HGB
Hauptabschlussübersicht	10 Jahre	§ 147 AO, § 257 HGB
I		
Initiativbewerbungen per Post	2 bis 6 Monate nach Absage zulässig ohne Einwilligung (Bewerber müssen gem. Art 13 DSGVO bei Eingang über Dauer informiert werden), ab Eingang etwa maximal drei Monate ohne Einwilligung	§ 26 BDSG, § 15 Abs. 4 AGG, Art. 13 DSGVO
Initiative Online-Bewerbungen	Normalerweise 2 Monate nach Absage ohne Einwilligung (Bewerber müssen gem. Art 13 DSGVO bei Eingang über Dauer informiert werden), ab Eingang etwa maximal drei Monate ohne Einwilligung	§ 26 BDSG, § 15 Abs. 4 AGG, Art. 13 DSGVO
Inventare (§ 240 HGB)	10 Jahre	§ 147 AO, § 257 HGB
Investitionszulage (Unterlagen)	6 Jahre	§ 147 AO, § 257 HGB
J		
Jahresabschluss mit Erläuterungen	10 Jahre	§ 147 AO, § 257 HGB
Journale für Hauptbuch oder Kontokorrent	10 Jahre	§ 147 AO, § 257 HGB
K		
Kalkulation und Kalkulationsunterlagen, wenn handels- oder steuerrechtlich relevant z.B. für Vorratsbewertung	10 Jahre	§ 147 AO, § 257 HGB
Kassenberichte	10 Jahre	§ 147 AO, § 257 HGB

Kassenbücher/-blätter	10 Jahre	§ 147 AO, § 257 HGB
Kassenzettel, (nicht erforderlich, wenn Tagessummenbons aufbewahrt werden)	10 Jahre	§ 147 AO, § 257 HGB
Kontaktanfragen über WEbformulare (insofern Belegfunktion)	10 Jahre	§ 147 AO, § 257 HGB
Kontaktanfragen über Webformulare (kein Fall von § 257 HGB, § 147 AO)	Nach Erledigung	Art. 6 Abs. 1 S. 1 lit. a, b, f; 17 DSGVO
Kontenpläne und Kontenplanänderungen	10 Jahre	§ 147 AO, § 257 HGB
Kontenregister	10 Jahre	§ 147 AO, § 257 HGB
Kontoauszüge	10 Jahre	§ 147 AO, § 257 HGB
Konzernabschluss (§ 290 HGB)	10 Jahre	§ 147 AO, § 257 HGB
Konzernlagebericht (§§ 290, 350 HGB)	10 Jahre	§ 147 AO, § 257 HGB
Kreditunterlagen, wenn Korrespondenz,	6 Jahre	§ 147 AO, § 257 HGB
Kreditunterlagen, wenn Buchungsbeleg	10 Jahre	§ 147 AO, § 257 HGB
Kundendatenerfassung via Web	10 Jahre	§ 147 AO, § 257 HGB
Kundendienst (insofern Belegfunktion)	10 Jahre	§ 147 AO, § 257 HGB
Kundendienst (Geschäftsbriefe, Mahnungen)	6 Jahre	§ 257 HGB
Kundendienst (kein Fall von § 257 HGB, § 147 AO)	Ende Konversation	Art. 6 Abs. 1 S. 1 lit. a, b, f; 17 DSGVO
L		
Lageberichte, wenn Bilanzunterlagen	10 Jahre	§ 147 AO, § 257 HGB
Lagerbuchführungen	10 Jahre	§ 147 AO, § 257 HGB
Lieferscheine	6 Jahre	§ 147 AO, § 257 HGB
Lieferscheine, sofern als Belegnachweis vor allem im Zusammenhang mit einer Rechnung	10 Jahre	§ 147 AO, § 257 HGB
Lohnbelege als Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Lohnlisten für Zwischen-, End- und Sonderzahlungen	6 Jahre	§ 147 AO, § 257 HGB
M		
Magnetbänder, wenn Grundbuch oder Konten- oder Belegfunktion	10 Jahre	§ 147 AO, § 257 HGB
Mahnbescheide und Mahnungen	6 Jahre	§ 147 AO, § 257 HGB
Mietunterlagen (nach Vertragsende), soweit Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Mobile Device Management Erfassungsdaten (nach Ausscheiden)	bei Rückgabe des Gerätes oder bei Neubeschaffung	
N		
Nachnahmebelege	10 Jahre	§ 147 AO, § 257 HGB
Nebenbücher	10 Jahre	§ 147 AO, § 257 HGB
Nutzerdaten (Verhalten, Zeiten, Kommunikation, nach Ende der Nutzung)	1 Jahr	
O		
Online-Rechnungen	10 Jahre	§ 147 AO, § 257 HGB
Organisationsunterlagen der EDV- Buchführung	10 Jahre	§ 147 AO, § 257 HGB
P		
Pachtunterlagen (nach Vertragsende), soweit Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Passwortmanager (nach Ende der Nutzung)	3 Monate	Art. 17 DS-GVO
Postgiroauszüge und Belege, wenn Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Preislisten	6 Jahre	§ 147 AO, § 257 HGB

Preislisten, wenn Bewertungs- oder Buchungsunterlagen	10 Jahre	§ 147 AO, § 257 HGB
Programmablaufbeschreibungen	10 Jahre	§ 147 AO, § 257 HGB
Programmverzeichnisse	10 Jahre	§ 147 AO, § 257 HGB
Projektdaten (nach Abschluss des Projektes)	1 Jahr	Art. 17 DSGVO
Protokolle, als Handelsbrief	6 Jahre	§ 147 AO, § 257 HGB
Prozessakten	10 Jahre	§ 147 AO, § 257 HGB
Prüfungsberichte des Abschlussprüfers	10 Jahre	§ 147 AO, § 257 HGB
Q		
Quittungen	10 Jahre	§ 147 AO, § 257 HGB
R		
Rechnungen an Unternehmer	10 Jahre	§ 147 AO, § 257 HGB
Registrierung / Nutzerkonto (insofern Belegfunktion, nach Ende der Geschäftsbeziehung)	10 Jahre	§ 147 AO, § 257 HGB
Registrierung / Nutzerkonto (Geschäftsbriefe, Mahnungen, nach Ende der Geschäftsbeziehung)	6 Jahre	§ 257 HGB
Registrierung / Nutzerkonto (kein Fall von § 257 HGB, § 147 AO, nach Ende der Geschäftsbeziehung))	3 Jahre	§§ 195, 199 BGB
Reisekostenabrechnung	10 Jahre	§ 147 AO, § 257 HGB
Repräsentationsaufwendungen (Unterlagen)	10 Jahre	§ 28 Abs. 3 RöV
S		
Sachkonten	10 Jahre	§ 147 AO, § 257 HGB
Saldenbilanzen	10 Jahre	§ 147 AO, § 257 HGB
Schadensunterlagen, wenn Bilanzunterlagen	10 Jahre	§ 147 AO, § 257 HGB
Scheck- und Wechselunterlagen,	6 Jahre	§ 147 AO, § 257 HGB
als Buchungsbeleg	10 Jahre	§ 147 AO, § 257 HGB
Schlüsselprotokolle (nach Ausscheiden, bei Mitarbeitern)	3 Monate	Art. 6 Abs. 1 S. 1 lit. b, 17 DSGVO
Schriftwechsel	6 Jahre	§ 147 AO, § 257 HGB
Server-Logdaten	9 Wochen	
Sonstige Beitragsabrechnungen des Arbeitgebers mit Sozialversicherungsträgern	Ablauf des auf die letzte Prüfung folgenden Kalenderjahres	§ 28f Abs. 1 SGB IV
Speicherbelegungsplan der EDV- Buchführung	10 Jahre	§ 147 AO, § 257 HGB
Spendenbescheinigungen	10 Jahre	§ 147 AO, § 257 HGB
Steuererklärungen	10 Jahre	§ 147 AO, § 257 HGB
Steuerbescheide	10 Jahre	§ 147 AO, § 257 HGB
T		
Telefondatenbank	1 Monat	Art. 6 Abs. 1 S. 1 lit. b, 17 DSGVO
Telefonkostennachweise, wenn Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Termindaten	2 Monate	Art. 6 Abs. 1 S. 1 lit. f, 17 DSGVO
U		
Überstundenlisten, wenn Lohnbelege	10 Jahre	§ 147 AO, § 257 HGB
Urlaubsdaten	2 Jahre	§§ 1, 3, 6 Abs. 2, 7 Abs. 3, 4 BUrlG
V		
Verbindlichkeiten (Zusammenstellungen)	10 Jahre	§ 147 AO, § 257 HGB
Vereinsdaten (insofern Belegfunktion)	10 Jahre	§ 147 AO, § 257 HGB

Verkaufsbücher	10 Jahre	§ 147 AO, § 257 HGB
Vermögensverzeichnis	10 Jahre	§ 147 AO, § 257 HGB
Versand- und Frachtunterlagen, wenn Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Versicherungspolicen,	10 Jahre	§ 147 AO, § 257 HGB
nach Ablauf der Versicherung	6 Jahre	§ 147 AO, § 257 HGB
Verträge, sonstige, soweit handels- und steuerrechtlich von Bedeutung und wenn Buchungsbelege	10 Jahre	§ 147 AO, § 257 HGB
Videoüberwachung	7 Tage	Art. 6 Abs. 1 S. 1 lit. f, 17 DSGVO
Visitenkarten (z.B. auf Messen bekommen)	Keine	
W		
Wareneingangs- und Warenausgangsbücher	10 Jahre	§ 147 AO, § 257 HGB
Warenwirtschaft & Rechnungsversand	10 Jahre	§ 147 AO, § 257 HGB
Webtracking und -analyse Daten	Anonymisierung nach Erhebung (z.B. Anonymize IP)	Art. 6 Abs. 1 S. 1 lit. f, 17 DSGVO
Wechsel	10 Jahre	§ 147 AO, § 257 HGB
Weiterbildungsdaten	3 Jahre oder 3 Monate nach Beendigung des Arbeitsverhältnisses	§ 195 BGB, § 26 BDSG
Widerrufs- und Garantiedaten (nach Abschluss des Falls)	3 Jahre	§§ 195, 199 BGB
Z		
Zahlungsanweisungen	10 Jahre	§ 147 AO, § 257 HGB
Zahlungsdaten (insofern Belegfunktion)	10 Jahre	§ 147 AO, § 257 HGB
Zollbelege	10 Jahre	§ 147 AO, § 257 HGB
Zugriffsregelungen bei EDV- Buchführung	10 Jahre	§ 147 AO, § 257 HGB
Zutrittsprotokolle	6 Monate	
Zwischenbilanz (bei Gesellschafterwechsel oder Umstellung des Wirtschaftsjahres)	10 Jahre	§ 147 AO, § 257 HGB