ZDH
ZENTRALVERBAND DES
DEUTSCHEN HANDWERKS

Leitfaden

Datenschutzrecht

Was Betriebe zu beachten haben

Stand: November 2020

Abteilung Organisation und Recht

DAS HANDWERK
DIE WIRTSCHAFTSMACHT. VON NEBENAN.

Vorwort

Seit dem 25. Mai 2018 gelten in allen Mitgliedstaaten der Europäischen Union neue Datenschutzregeln. Mit der Reform soll sichergestellt werden, dass in allen Mitgliedstaaten derselbe Datenschutzstandard besteht. Da in Deutschland bereits hohe Anforderungen an den Datenschutz gelten, führen die neuen Vorschriften zwar zu zahlreichen formellen Änderungen. Eine inhaltliche Verschärfung der Anforderungen geht mit der Reform jedoch insgesamt nicht einher.

Handwerksbetriebe müssen sicherstellen, dass sie die erforderlichen Anpassungen vornehmen. Der vorliegende Leitfaden thematisiert die für die handwerkliche Praxis wichtigsten Aspekte und Fragen. Er bietet neben rechtlichen Erklärungen zahlreiche Beispielsfälle, Checklisten und Muster, die in der betrieblichen Praxis genutzt werden können.

Der Leitfaden zielt darauf ab, Handwerksbetrieben einen vertieften Überblick sowie das notwendige Rüstzeug zu geben, die jeweiligen betrieblichen Abläufe an die Anforderungen des neuen Datenschutzrechts anzupassen. Eine rechtlich abschließende und verbindliche Beratung darf und kann der Leitfaden nicht leisten. Für spezielle Einzelfragen zu individuellen Situationen des Betriebs sollten die entsprechenden Experten der Handwerksorganisationen hinzugezogen werden.

Inhaltsverzeichnis

ANLAGEN

Anlage 6: Muster: Technische und organisatorische Maßnahmen

Anlage 7: Muster Benennung eines/r betrieblichen Datenschutzbeauftragten

Anlage 8: Musterformulierungen für Auftragsverarbeitungsvertrag

Anlage 9: Einwilligungserklärung für die Veröffentlichung von Mitarbeiterfotos auf der Betriebswebsite

Anlage 10 Muster Information der Beschäftigten bei Aufnahme der Tätigkeit

Anlage 11 Muster Information des Ausbildungsbetriebs an den Auszubildenden bei Abschluss des Lehrvertrags

Anlage 12 Muster Verarbeitungsverzeichnis bezüglich Lohnabrechnung

Anlage 13 Muster Verarbeitungsverzeichnis bezüglich Personalführung

Anlage 14 Muster Verpflichtung zur Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten

Anlage 15 Muster Einwilligungserklärung für den Einsatz von Videokameras in nicht öffentlich zugänglichen Betriebsräumlichkeiten

Anlage 16 Musterinformation Videoüberwachung

Anlage 17 Aufbewahrungs- und Löschfristen

Anlage 18 Musterformulierung: Information der Kunden über Weiterleitung der Kundendaten an den Betriebsnachfolger (inhabergeführte Betriebe/Personengesellschaften)

Anlage 19 Musterformulierung für Handwerksbetriebe der Gesundheitshandwerke: Einwilligung zur Übertragung von Kundendaten an den Käufer

Anlage 20 Musterformulierung: Einwilligung zur Kontaktaufnahme per E-Mail, Telefon, Fax (Werbung)

1. Zulässige Datenverarbeitung ohne Einwilligung

Wann ist die Nutzung von Daten erlaubt?

Eine Datennutzung ist nur zulässig, wenn

- eine gesetzliche Vorschrift sie erlaubt oder
- derjenige, dessen Daten verarbeitet werden sollen, in die Nutzung von Daten einwilligt (siehe hierzu Kapitel 2: Anforderungen an die datenschutzrechtliche Einwilligung).

Gesetzliche Erlaubnis

Vorschriften, die eine Datennutzung erlauben, finden sich hauptsächlich in Artikel 6 der Europäischen Datenschutz-Grundverordnung (DSGVO). Diese Regelungen werden durch die §§ 22, 24, 26 des Bundesdatenschutzgesetzes (BDSG) ergänzt.

Gemäß Art. 6 DSGVO ist eine Datenverarbeitung ohne Einwilligung zulässig, wenn die Verarbeitung

- zur **Erfüllung eines Vertrags** erforderlich ist (z.B. Adresse des Kunden, um den Auftrag vor Ort beim Kunden ausführen zu können).
- zur Durchführung **vorvertraglicher Maßnahmen** erforderlich ist (z.B. E-Mail-Adresse, um dem Kunden nach seinem Wunsch einen Kostenvoranschlag senden zu können).
- zur **Wahrung berechtigter Interessen** des Handwerksbetriebs oder eines Dritten erforderlich ist und die Interessen der betroffenen Person nicht überwiegen (z.B. die Auswertung der Kundendatei, um bestimmte Kunden zielgerichtet mit Werbung anzusprechen).

Beachte: Die Datennutzung zur Direktwerbung ist zulässig. Allerdings dürfen Betroffene der Werbung jederzeit widersprechen (Art. 21 Absatz 2 DSGVO). Für **Werbung per E-Mail** ist weiterhin eine Einwilligung erforderlich.

Die Verarbeitung personenbezogener Daten von Arbeitnehmern konkretisiert § 26 BDSG. Hiernach ist eine Verarbeitung zulässig, wenn es

- zur **Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses** erforderlich ist (z.B. Speicherung von Lohnunterlagen und Krankheitstagen).

- zur **Ausübung der Interessensvertretung** der Beschäftigten erforderlich ist (z.B. Weiterleitung von Arbeitnehmerdaten an den Betriebsrat).

Verwendung von Gesundheitsdaten

Gesundheitsdaten (z.B. Dioptrienzahl, Gehörschädigung etc.) gelten als besonders schutzwürdige Daten (Art. 9 DSGVO). Für Betriebe der Gesundheitshandwerke folgt die Berechtigung zur Verarbeitung von Gesundheitsdaten aus § 22 Abs. 1 Nr. 1 b) BDSG. Diese Vorschrift erlaubt die Verarbeitung von Gesundheitsdaten

- zum Zweck der Gesundheitsvorsorge.

- zur Versorgung oder Behandlung im Gesundheits- oder Sozialbereich.

- wenn es für einen Vertrag zwischen der betroffenen Person und einem Angehörigen eines Gesundheitsberufs erforderlich ist.

2. Anforderungen der datenschutzrechtlichen Einwilligung

Wann ist eine Datennutzung erlaubt?

Eine Datennutzung ist nur zulässig, wenn

- eine gesetzliche Vorschrift sie erlaubt oder
- derjenige, dessen Daten verarbeitet werden sollen, in die Datennutzung einwilligt.

Eine rechtmäßige Datennutzung setzt deshalb entweder eine gesetzliche Erlaubnis (siehe hierzu Kapitel 1 „Zulässige Datenverarbeitung ohne Einwilligung“, S. 4) oder eine Einwilligung des Betroffenen voraus.

Damit eine Einwilligung wirksam ist, müssen die gesetzlichen Anforderungen an eine Einwilligungserklärung erfüllt sein. Für Betriebe gelten die Vorschriften der Europäischen Datenschutzgrundverordnung (Artikel 7 DSGVO), die durch das Bundesdatenschutzgesetz (§ 51 BDSG) ergänzt werden.

Einwilligungen müssen freiwillig sein

Eine Einwilligung ist nur dann rechtmäßig, wenn derjenige, der die Einwilligung erklärt, dies freiwillig tut. Jede Form von Druck, Zwang oder Verpflichtung führt deshalb zur Unwirksamkeit der Einwilligung. Eine Einwilligung gilt unter anderem bereits als unfreiwillig, wenn der Abschluss eines Vertrags oder die Erbringung einer Leistung von der Abgabe der Einwilligungserklärung abhängig gemacht wird und der Kunde keine Möglichkeit hat, die Leistung auf andere Weise zu erlangen.

Besonderheiten bei Minderjährigen

Die Wirksamkeit einer Einwilligung ist nicht vom Alter des Einwilligenden abhängig. Insofern spielt es an sich keine Rolle, ob es sich um einen Minderjährigen oder einen Volljährigen handelt. Für die Wirksamkeit der Einwilligung ist allein die Einsichtsfähigkeit des Einwilligenden in die Tragweite seiner Erklärung maßgeblich. Der Einwilligende muss erkennen können, welche Folgen die Einwilligung für ihn hat.

Ob Minderjährige diese Einsichtsfähigkeit besitzen, kann nicht pauschal beurteilt werden, sondern richtet sich nach den Umständen des Einzelfalls. Da die Einsichtsfähigkeit eines Minderjährigen nicht in jedem Fall mit abschließender Sicherheit beurteilt werden kann, empfiehlt es sich in der Praxis, bei Minderjährigen stets die Einwilligungserklärung der Erziehungsberechtigten einzuholen.

Textform

Einwilligungen müssen – anders als früher – nicht mehr schriftlich erklärt werden. Eine mündliche Einwilligung ist deshalb in gleicher Weise wirksam. Allerdings sollte die Einwilligungserklärung allein aus Beweis- und Dokumentationsgründen stets in Textform eingeholt werden.

Die gewählte Form der Einwilligung ist zugleich Maßstab für den Fall, dass die Einwilligung widerrufen wird. Wurde die Einwilligung mündlich erteilt, muss ein mündlich erklärter Widerruf akzeptiert werden. Die Dokumentation mündlicher Erklärungen ist allerdings aufwändig, fehleranfällig und für effiziente Betriebsabläufe nicht zu empfehlen.

Welchen Inhalt müssen Einwilligungserklärungen haben?

Die gesetzlichen Vorschriften geben klare Mindestanforderungen an Einwilligungen vor.

- Der Datenverarbeiter muss seine Identität offenlegen (Angabe des Namens bzw. der Firma).
- Es muss dargelegt werden, welche Daten erhoben werden (z.B. Adressdaten, Kontodaten).
- Es muss der Zweck genannt werden, für den die Daten verarbeitet werden (z.B. Werbung, Weitergabe an Dritte).
- Hinweis auf das Widerrufsrecht: Der Einwilligende hat die Einwilligung freiwillig erklärt und kann sie jederzeit mit Wirkung für die Zukunft widerrufen. Es ist anzugeben, in welcher Form (Textform) und an welche Adresse (Postanschrift, E-Mail-Adresse) der Widerruf zu richten ist.

Die Angaben müssen verständlich und in klarer, einfacher Sprache formuliert werden. Sie müssen so konkret und so umfassend sein, dass sich der Einwilligende darüber ein Bild machen kann, was mit seinen Daten passiert.

Optische Gestaltung

Die Einwilligungserklärung ist optisch so zu gestalten, dass sie ins Auge fällt und vom Einwilligenden wahrgenommen wird. Dies ist vor allem dann wichtig, wenn die Einwilligungserklärung zusammen mit anderen Informationen (z.B. Allgemeinen Geschäftsbedingungen) in einem einzigen Text vorgelegt wird. Die erforderliche optische Abhebung ist beispielsweise durch eine Einrahmung, einen Fettdruck, eine andere Farbe oder durch eine andere Schriftgröße möglich.

Aktive Erklärung erforderlich

Die Einwilligung muss aktiv erklärt werden und sollte durch eine eindeutige bestätigende Handlung erfolgen. Dies kann – abgesehen von einer unterschriebenen Einwilligung – z.B. durch Anklicken eines Kästchens beim Besuch einer Internetseite geschehen. Stillschweigen, das bloße Hinnehmen bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen keine Einwilligung dar.

Soll die datenschutzrechtliche Einwilligung gemeinsam mit weiteren Erklärungen abgegeben werden, so sollte für jede Erklärung eine gesonderte Unterzeichnung oder ein gesondertes Anklicken vorgesehen werden. Dies bietet sich allein aus Beweiszwecken an. Eine einzige Unterschrift/Bestätigung für das gesamte Dokument birgt dagegen das Risiko der Unzulässigkeit und ist deshalb nicht zu empfehlen.

Wie lange gilt eine Einwilligung?

Obwohl die gesetzlichen Vorschriften keine zeitliche Geltungsdauer vorsehen, wird in der Praxis davon ausgegangen, dass erklärte Einwilligungen nicht unbeschränkt gültig sind.

Eine Einwilligung kann nur herangezogen werden, solange derjenige, der eingewilligt hat, vernünftiger Weise mit einer Verarbeitung seiner Daten rechnen muss. Dies kann je nach Fall unterschiedlich sein. Wer seine Einwilligung zum Erhalt von Werbung zu den regelmäßigen Sonderaktionen seines Optikers erklärt hat, muss nicht damit rechnen, dass er nach mehreren Jahren erstmals oder erneut Werbung erhält. Anders verhält es sich bei Werbung für Autos, die für gewöhnlich in längeren Zeitabständen erfolgt.

Weiterführende Unterlagen:

Anlage 1: Muster einer Einwilligungserklärung

3. Formelle Pflichten von Betrieben – Ein Überblick

Welchen Zweck verfolgen die Pflichten?

Das Datenschutzrecht räumt Personen, deren Daten von Betrieben genutzt werden, zahlreiche Rechte ein. Mithilfe dieser Rechte soll erreicht werden, dass diese Betroffenen Einfluss auf den Umgang und die Verbreitung ihrer Daten haben.

Für Betriebe, die Daten verarbeiten, bestehen kehrseitig gewisse Anforderungen an die Datennutzung. Wer Daten z.B. seiner Kunden und Geschäftspartner nutzen möchte, muss diese überwiegend formalen Anforderungen erfüllen. Die Pflichten von Betrieben und die Rechte von Betroffenen sind in den Artikeln 12 bis 22 der Datenschutz-Grundverordnung (DSGVO) geregelt. Die Vorschriften werden durch die §§ 32 bis 37 des Bundesdatenschutzgesetzes (BDSG) ergänzt.

Betriebe, die Daten nutzen, werden vom Gesetz als „Verantwortliche“ bezeichnet, weil sie die Datennutzung verantworten und für Datenpannen einstehen müssen. Ihre Pflichten sind im Einzelnen:

Transparenzgebot (Art. 12 DSGVO)

Art. 12 regelt den Umgang mit Anfragen des Betroffenen und in welcher Form Anfragen zu beantworten sind. Der Verantwortliche hat der betroffenen Person sämtliche Informationen und alle Mitteilungen auf präzise, transparente, verständliche und leicht zugängliche Weise in einer klaren und einfachen Sprache unverzüglich zu übermitteln. Obwohl auch eine mündliche Information zulässig ist, ist in der Praxis die Textform allein aus Beweisgründen zu empfehlen. Hierbei spielt es keine Rolle, ob der Text in Papierform oder elektronisch übermittelt wird.

Informationspflichten (Art. 13 und 14 DSGVO)

Art. 13 regelt, welche Informationen der Verantwortliche dem Betroffenen zu erteilen hat, wenn er beim Betroffenen Daten erhebt. Art. 14 bestimmt die Informationspflichten, wenn die Daten nicht bei der betroffenen Person selbst, sondern bei einem Dritten erhoben werden. Siehe hierzu ausführlich Kapitel 4 „Informationspflichten bei Erhebung personenbezogener Daten“.

Auskunftsrecht (Art. 15 DSGVO)

Betroffene haben das Recht, vom datenverarbeitenden Betrieb eine Bestätigung zu verlangen, ob über sie personenbezogene Daten gespeichert sind und verarbeitet werden. Ist das

der Fall, hat der Betrieb Auskunft über diese Daten, deren Herkunft sowie weitere Informationen zu erteilen. In der Praxis werden solche Auskunftsanfragen i.d.R. von Kunden auf Betriebe zukommen (siehe hierzu Kapitel 5 „Erteilung von Auskünften“).

Recht auf Berichtigung (Art. 16 DSGVO)

Sind personenbezogene Daten falsch, nicht mehr aktuell oder unvollständig, haben die betroffenen Personen gemäß Art. 16 ein Recht auf Berichtigung. Der verantwortliche Datenverarbeiter muss die unrichtigen oder unvollständigen Daten unverzüglich korrigieren.

Recht auf Löschung (Art. 17 DSGVO)

Nach Art. 17 haben Betroffene das Recht, die Löschung ihrer Daten zu verlangen, wenn einer der gesetzlich geregelten Löschungsgründe vorliegt. Ein solcher Grund liegt vor, wenn:

- die Aufbewahrung der Daten für den Zweck, zu dem sie ursprünglich erhoben wurden, nicht mehr erforderlich ist,
- die Daten unrechtmäßig verarbeitet wurden,
- der Betroffene seine Einwilligung für eine weitere Speicherung widerrufen hat.

Selbst wenn einer der vorgenannten Gründe vorliegt, dürfen Daten aber nicht gelöscht werden, wenn gesetzliche Aufbewahrungsfristen bestehen und der Verantwortliche damit zur Aufbewahrung verpflichtet ist (z.B. bei rentenrelevanten Unterlagen von Mitarbeitern).

Anstelle einer Löschung tritt die sog. Einschränkung der Verarbeitung gemäß § 35 BDSG, wenn die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse des Betroffenen an der Löschung als gering anzusehen ist (siehe hierzu unten).

Recht auf Vergessenwerden (Art. 17 DSGVO)

Eine besondere Form des Löschungsanspruchs ist das „Recht auf Vergessenwerden“. Dieses Recht bezieht sich auf Daten, die veröffentlicht wurden und zielt insbesondere auf Veröffentlichungen im Internet ab. Für Handwerksbetriebe dürfte dies in der Praxis jedoch keine große Rolle spielen.

Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Mit dem Recht auf Einschränkung der Verarbeitung können Betroffene in bestimmten Fällen erwirken, dass der Datenverarbeiter ihre Daten sperrt und somit nicht weiterverarbeiten darf. Dies gilt u.a. für den Fall, dass

- die Richtigkeit gespeicherter Daten bestritten wird und die Datennutzung für die Dauer der Überprüfung der Richtigkeit ausgesetzt werden soll,

- die Datenverarbeitung unrechtmäßig ist und der Betroffene anstatt der Löschung die Nutzungseinschränkung bevorzugt.

Pflicht zur Datenübertragung (Art. 20 DSGVO)

Das Recht auf Datenübertragung gibt Betroffenen unter bestimmten Voraussetzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen Dateiformat zu erhalten. Der Betroffene hat damit das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen“. Die Regelung soll den Wechsel zu einem anderen Anbieter insbesondere bei sozialen Netzwerken oder Verträgen mit Energieversorgern, Banken und Versicherungen erleichtern. Für Handwerksbetriebe wird dieses Recht jedoch keine Praxisrelevanz haben.

Widerspruchsrecht (Art. 21 DSGVO)

Betroffenen steht ein Widerspruchsrecht gegen eine Verarbeitung ihrer Daten zum Zweck der Direktwerbung zu. Obwohl die Nutzung von Daten zur Direktwerbung zulässig ist, können betroffene Personen hiergegen jederzeit und ohne Angabe von Gründen widersprechen. Nach erfolgtem Widerspruch dürfen die Daten nicht mehr zur Direktwerbung genutzt werden.

Dokumentationspflicht (Art. 30 DSGVO)

Handwerksbetriebe sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „Verzeichnis von Verarbeitungstätigkeiten“ zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe im Betrieb gegeben werden. Erweist sich eine beabsichtigte Datennutzung als risikoreich, ist zusätzlich eine „Datenschutz-Folgenabschätzung“ nach Art. 35 DSGVO vorzunehmen. Siehe hierzu ausführlich Kapitel 6 „Dokumentationspflicht“.

4. Informationspflichten bei Erhebung personenbezogener Daten

Transparenz durch Informationen

Personen, deren Daten von einem anderen verarbeitet werden, sollen im Vorlauf zur Datenverarbeitung informiert werden. Insbesondere sollen sie erfahren, welche Daten über sie erhoben und zu welchem Zweck sie genutzt werden. Um diese Transparenz herzustellen, sind Betriebe verpflichtet, den jeweils betroffenen Personen zahlreiche Informationen über die beabsichtigte Datennutzung zu erteilen. Welche Informationen dies im Einzelnen sind, ist in den Art. 13 und 14 der Europäischen Datenschutz-Grundverordnung (DSGVO) aufgelistet, die durch §§ 32 und 33 des Bundesdatenschutzgesetzes (BDSG) ergänzt werden.

Bei den Informationspflichten sind drei Situationen zu unterscheiden:

- Die Daten werden bei der Person, deren Daten verarbeitet werden sollen, direkt erhoben.
- Die Daten, die verarbeitet werden sollen, werden nicht bei der betroffenen Person selbst, sondern von einem Dritten erhoben.
- Der Datenverarbeiter hat die Daten bereits vorliegen und möchte die Daten zu einem anderen Zweck nutzen, als zu dem, zu dem sie ursprünglich bei der betroffenen Person erhoben wurden.

Erhebung personenbezogener Daten beim Betroffenen selbst (Art. 13 DSGVO)

Werden personenbezogene Daten bei Betroffenen direkt erhoben (z.B. von Kunden oder Besuchern von Webseiten), müssen diesen folgende Informationen mitgeteilt werden:

- **Identität des Verantwortlichen**: Name und Kontaktdaten des Datenverarbeiters (bei juristischen Personen zudem Name des Vertreters, z.B. Name des Geschäftsführers).
- **Kontaktdaten des Datenschutzbeauftragten (DSB):** Dies gilt nur, sofern ein DSB bestellt ist. Der Name des DSB ist hierbei nicht zwingend zu nennen. Zur Frage wann ein DSB zu bestellen ist, siehe Kapitel 7 „Der Datenschutzbeauftragte“.
- **Verarbeitungszweck der Datennutzung**: Z.B. für Werbemaßnahmen oder zur Abwicklung eines Vertrags.

- **Rechtsgrundlage der Datenverarbeitung:** Entweder Benennung der gesetzlichen Norm, die die Datenerhebung erlaubt (siehe hierzu Kapitel 1 „Zulässige Datenverarbeitung ohne Einwilligung“) oder Einwilligung des Betroffenen (siehe hierzu Kapitel 2 „Anforderungen der datenschutzrechtlichen Einwilligung“). Bei einer Einwilligung ist zusätzlich der Hinweis auf das **Recht zum Widerruf der Einwilligung** erforderlich.

- **Empfänger** oder Kategorien von Empfängern der Daten: Gilt nur, wenn die Daten an Dritte weitergeleitet werden. Z.B. Weitergabe von Daten an die Creditreform.

- **Dauer der Verarbeitung** oder Dauer der Datenspeicherung: In der Regel dauert die Datennutzung an, bis der Zweck der Datenverarbeitung erreicht ist.

- **Rechte der Betroffenen**: Z.B. Recht auf Auskunft, Berichtigung, Löschung (siehe hierzu Kapitel 3 „Formelle Pflichten – Ein Überblick**“**).

- Hinweis auf das **Beschwerderecht bei der Aufsichtsbehörde.**

- Hinweis, ob die **Bereitstellung der Daten** für den Abschluss oder die Abwicklung eines Vertrags **erforderlich ist**: Z.B. Adresse des Kunden, wo der Auftrag zur Reparatur durchgeführt werden soll.

Erhebung personenbezogener Daten bei Dritten (Art. 14 DSGVO)

Werden personenbezogene Daten nicht beim Betroffen selbst, sondern bei einem Dritten oder aus öffentlichen Quellen erhoben, müssen zunächst dieselben Angaben gemacht werden, wie bei der Erhebung beim Betroffenen selbst.

Zusätzlich sind dem Betroffenen zwei weitere Informationen zu erteilen:

- Welche **Kategorien** personenbezogener Daten erhoben werden: Werden z.B. einfache Adressdaten oder besonders sensible Daten wie z.B. Gesundheitsdaten erhoben?

- Aus welcher **Quelle** die personenbezogenen Daten stammen und ob es sich dabei um eine öffentlich zugängliche Quelle handelt.

Zweckänderung

Für den Fall, dass der Verantwortliche die Daten bereits vorliegen hat und für einen anderen Zweck weiterverarbeiten möchte, muss er die betroffenen Personen vor der Weiterverarbeitung über folgende Aspekte informieren:

- den neuen Zweck der Verarbeitung,
- die Dauer der Verarbeitung (siehe oben bei Erhebung beim Betroffenen),
- die Rechte des Betroffenen (siehe oben bei Erhebung beim Betroffenen),
- Beschwerderecht (siehe oben bei Erhebung beim Betroffenen).

Wann ist zu informieren?

Im Fall der Datenerhebung beim Betroffenen müssen die Informationen im Zeitpunkt der Datenerhebung mitgeteilt werden. Werden die Daten nicht beim Betroffenen erhoben, muss der Verantwortliche die Informationen innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat erteilen. Bei einer Zweckänderung ist der Betroffene vor der Verwendung der Daten zum neuen Zweck zu unterrichten.

Gibt es Ausnahmen von der Informationspflicht?

Die Information des Betroffenen ist nicht erforderlich, soweit dieser bereits Kenntnis über die einzelnen Angaben der Datenverarbeitung hat.

Werden die Daten bei einem Dritten erhoben, darf die Information zudem unterbleiben, wenn die Informationserteilung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.

Sind Formvorschriften zu beachten?

Die Informationen müssen nach Maßgabe von Art. 12 Abs. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erteilt werden.

Die Übermittlung der Informationen sollte grundsätzlich in Textform erfolgen. Obwohl auch eine mündliche Information möglich ist, sollte in der Praxis allein aus Beweisgründen die Textform gewählt werden. Hierbei spielt es keine Rolle, ob der Text in Papierform oder elektronisch übermittelt wird.

Drohen bei Verstößen Sanktionen?

Verstöße gegen die datenschutzrechtlichen Informationspflichten können gemäß Art. 83 Abs. 5 DSGVO Strafen in Höhe von bis zu 20 Mio. EUR oder vier Prozent des Weltjahresumsatzes ausgesprochen werden.

5. Erteilung von Auskünften

Das Auskunftsrecht

Das Datenschutzrecht gewährt Personen, deren Daten verarbeitet werden, umfassende Rechte (siehe hierzu allgemein Kapitel 3 „Formelle Pflichten – Ein Überblick“). Eines dieser Rechte ist das Auskunftsrecht. Das Auskunftsrecht ist in Art. 15 der Europäischen Datenschutz-Grundverordnung (DSGVO) geregelt und wird durch § 34 Bundesdatenschutzgesetz (BDSG) ergänzt. Hiernach haben Betroffene das Recht, vom datenverarbeitenden Betrieb eine Bestätigung zu verlangen, ob über sie personenbezogene Daten gespeichert sind oder verarbeitet werden. Ist das der Fall, hat der Betrieb Auskunft über diese Daten, deren Herkunft sowie weitere Informationen zu erteilen. In der Praxis werden solche Auskunftsanfragen i.d.R. von Kunden auf Betriebe zukommen.

Auskunftsersuchen

Die Erteilung der Auskunft setzt zunächst ein Auskunftsersuchen voraus. Die Anfrage kann mündlich, schriftlich oder elektronisch (z.B. per E-Mail) gestellt werden. Zudem sollte das Auskunftsersuchen auf bestimmte Daten oder Informationen präzisiert sein. Dies ist jedoch keine Pflicht. Es kann auch pauschal Auskunft über alle gespeicherten Daten verlangt werden.

Inhalt der Auskunft

Verlangt der Antragsteller eine pauschale Auskunft über seine Daten, sind sämtliche vom Gesetz vorgesehene Informationen zu erteilen. Dies sind im Einzelnen:

- Alle über den Betroffenen gespeicherten Daten (z.B. Name, Anschrift, E-Mail-Adresse, Bankverbindung).
- Die Kategorien der Daten, die verarbeitet werden (z.B. Vertragsdaten, Adress- und Kontaktdaten).
- Die Bezeichnung der Datei (z.B. Kundendatei, Neukunden).
- Angaben über die Herkunft der Daten (z.B. Daten wurden beim Betroffenen selbst erhoben, Daten wurden von einem Dritten gekauft).
- Die Empfänger, an die die Daten weitergeleitet wurden.

- Die geplante Dauer, für die die Daten gespeichert werden (i.d.R. sind Daten so lange zu speichern, bis sie nicht mehr benötigt werden).

- Der Zweck der Speicherung, d.h. aus welchem Grund werden die Daten gespeichert? (Z.B. Nutzung zur Direktwerbung).

Zusätzlich zu den vorgenannten Angaben über die gespeicherten Daten, sind u.a. weitere Informationen zu den Rechten des Betroffenen zu erteilen:

- Hinweis auf das Bestehen eines Rechts auf Berichtigung oder Löschung (Art. 16 DSGVO) oder auf eine Einschränkung der Verarbeitung (Art. 18 DSGVO). Siehe hierzu Kapitel 3 „Formelle Pflichten – Ein Überblick“.

- Das Bestehen eines Beschwerderechts des Betroffenen bei der Datenschutzaufsichtsbehörde.

Verfahren der Auskunftserteilung

Der Betrieb hat sich vor Erteilung der Auskunft über die Identität des Antragstellers zu vergewissern. Der Antragsteller und die betroffene Person, deren Daten gespeichert sind, müssen identisch sein. Wie die Identitätsprüfung erfolgt, bestimmt der Betrieb.

Wie ist die Auskunft zu erteilen?

Die Auskunft soll in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen (Art. 12 DSGVO).

Der Betrieb hat dem Antragsteller eine Kopie der Daten zur Verfügung zu stellen. Stellt die betroffene Person den Antrag elektronisch, sind die Informationen in einem gängigen elektronischen Format auszuhändigen. Alternativ kann dem Antragsteller auch ein unmittelbarer Fernzugriff auf die Daten ermöglicht werden.

Kann die Auskunft insgesamt verweigert werden?

Neben einer Verweigerung wegen überwiegender Geschäftsgeheimnisse kommt eine vollständige Verweigerung der Auskunft nur in Betracht, wenn die Auskunft unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Wird die Auskunft verweigert, ist dies zu begründen.

In welchem Zeitrahmen ist die Auskunft zu erteilen?

Die Auskunft ist unverzüglich, spätestens innerhalb von vier Wochen, zu erteilen.

Kosten der Auskunft

Die Auskunftserteilung ist für den Betroffenen kostenlos. Verlangt der Antragsteller jedoch mehr als eine Kopie, kann ein entsprechendes Entgelt für die entstehenden Kosten verlangt werden.

Muster zur Auskunftserteilung

Ein Muster zur Erteilung einer Auskunft an einen Kunden befindet sich in **Anlage 3**.

6. Dokumentationspflicht

Weshalb ist eine Dokumentation nötig?

Handwerksbetriebe, die personenbezogene Daten verarbeiten, sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „Verzeichnis von Verarbeitungstätigkeiten“ zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe im Betrieb gegeben werden. Auf Grundlage dieser Übersicht sollen sich Betriebsinhaber über das Ausmaß und die Intensität der betrieblichen Datenverarbeitung bewusst werden.

Die Pflicht zur Dokumentation der Datenverarbeitungsprozesse sowie die konkreten Anforderungen an die Dokumentation sind in Artikel 30 der Europäischen Datenschutz-Grundverordnung (DSGVO) geregelt.

Was ist zu dokumentieren?

Nach Art. 30 DSGVO sind alle Tätigkeiten zu dokumentieren, bei denen personenbezogene Daten verarbeitet werden. Solche Tätigkeiten können in den unterschiedlichsten betrieblichen Situationen vorkommen (z.B. Erstellung und Veränderung der Kundendatei, Verwaltung der Mitarbeiterakten, Verwendung einer Kamera im Betrieb).

Wie ist der Ablauf der Dokumentation?

Schritt 1: Risikobewertung

Im ersten Schritt ist zu bewerten, ob die Datenverarbeitung ein hohes oder geringes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind (z.B. betriebliche Videoüberwachung mit Blick auf eine öffentliche Straße). Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten, ethnische Herkunft, religiöse Zugehörigkeit) umfangreich verarbeitet werden. Dies ist bei Handwerksbetrieben gewöhnlich nicht der Fall. Ausnahmen sind in der Regel jedoch Betriebe der Gesundheitshandwerke oder große Betriebe mit vielen Mitarbeitern, die in der Personalabteilung solche Daten umfangreich verarbeiten.

Sollte ausnahmsweise ein hohes Risiko bestehen, ist eine „Datenschutz-Folgenabschätzung“ vorzunehmen. Die Anforderungen dieser Folgenabschätzung richten sich nach Art. 35 DSGVO und umfassen folgende Prüfungspunkte:

- eine Beschreibung der geplanten Verarbeitungsvorgänge,

- eine Beschreibung der Zwecke der Verarbeitung,
- eine Bewertung der Notwendigkeit der Verarbeitungsvorgänge,
- eine Bewertung der Risiken für die Personen, deren Daten verarbeitet werden sollen,
- eine Beschreibung der Maßnahmen, die zur Bewältigung der Risiken vorgesehen werden.

Schritt 2: Erstellen des Verarbeitungsverzeichnisses

Art. 30 DSGV zählt die Punkte auf, die in einem Verarbeitungsverzeichnis enthalten sein müssen. Dies sind im Einzelnen:

- **Name und die Kontaktdaten des Betriebs** (bei juristischen Personen zudem Name des Vertreters, z.B. Name des Geschäftsführers)
- **Name und Kontaktdaten des Datenschutzbeauftragten** (DSB): Nur erforderlich, wenn ein DSB bestellt wurde (zur Frage wann ein DSB zu bestellen ist, siehe Kapitel 7 „Der Datenschutzbeauftragte).
- **Zwecke der Verarbeitung**: Z.B. für Werbemaßnahmen oder zur Abwicklung eines Vertrags.
- Beschreibung der **Kategorien betroffener Personen**: Z.B. Kunden, Mitarbeiter, Zulieferer etc.
- Beschreibung der **Kategorien personenbezogener Daten**: Werden z.B. einfache Adressdaten oder besonders sensible Daten wie z.B. Gesundheitsdaten erhoben?
- **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden: Gilt nur, wenn die Daten an Dritte weitergeleitet werden (z.B. Weitergabe von Daten an die Creditreform).
- Wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien: In der Regel gilt, dass Daten zu löschen sind, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden.
- Wenn möglich, eine Beschreibung der **technischen und organisatorischen Maßnahmen** (siehe hierzu nachfolgend).

Technische und organisatorische Maßnahmen

Betriebe sind verpflichtet, Maßnahmen auf dem Stand der Technik zu ergreifen, um den Risiken zu begegnen, die mit der Datenverarbeitung einhergehen. § 64 Bundesdatenschutzgesetz zählt zahlreiche Maßnahmen auf, die zu berücksichtigen sind. Diese lassen sich thematisch auf folgende Kernmaßnahmen zusammenfassen:

- **Vertraulichkeit der Datenverarbeitung (u.a. Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle)**
  Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden (z.B. Abschließen des Serverraums).

- **Integrität der Datenverarbeitung (u.a. Eingabekontrolle/ Verarbeitungskontrolle)**
  Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (z.B. Verwendung individueller Benutzernamen).

- **Verfügbarkeitskontrolle**
  Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können (z.B. Installierung von Geräten zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen).

- **Trennungsgebot**
  Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (z.B. Trennung von Daten verschiedener Auftraggeber).

Muster eines Verarbeitungsverzeichnisses

Ein Muster für ein Verarbeitungsverzeichnis ist als **Anlage 4** beigefügt. **Anlage 5** enthält ein ausgefülltes Beispiel. Zudem befindet sich in **Anlage 6** eine Checkliste möglicher heranzuziehender technischer und organisatorischer Maßnahmen.

7. Der betriebliche Datenschutzbeauftragte (DSB)

Gesetzliche Verpflichtung

Die Anforderungen an den betrieblichen Datenschutzbeauftragten ergeben sich aus den Artikeln 37 bis 39 der Europäischen Datenschutz-Grundverordnung (DSGVO) und § 38 Bundesdatenschutzgesetz (BDSG).

Müssen Gesundheitshandwerker einen Datenschutzbeauftragten bestellen?

Ein Datenschutzbeauftragter ist zu bestellen, wenn ein Betrieb Gesundheitsdaten umfangreich verarbeitet (§ 38 BDSG, Art. 35 DSGVO). Zwar verarbeiten Gesundheitshandwerker Gesundheitsdaten, jedoch erfolgt dies nicht in umfangreicher Weise. So wird lediglich ein Gesundheitsdatum pro Kunde verarbeitet. Im Vergleich zu Krankenhäusern oder großen Arztpraxen, die sowohl unterschiedliche Gesundheitsdaten als auch eine weitaus höhere Anzahl an Patienten betreuen, wird der geringe Umfang deutlich. Für Gesundheitshandwerker gelten somit i.d.R. dieselben Regelungen wie für andere Handwerksbetriebe.

Welcher Handwerksbetrieb muss einen Datenschutzbeauftragten benennen?

Sind im Betrieb mindestens 20 Personen angestellt, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist ein DSB zu benennen. Automatisierte Verarbeitung ist z.B. die Nutzung digitaler Kundendateien oder die Verwendung von Kundendaten auf einem Tablet-PC oder Smartphone. Als „ständig befasst“ gelten nur solche Mitarbeiter, deren alltägliche Kerntätigkeit die Verarbeitung von Daten ist. Dies ist z.B. bei Mitarbeitern der Lohnbuchhaltung oder der Personalabteilung der Fall. Mitarbeiter, die lediglich die Daten zur Ausübung ihrer handwerklichen Tätigkeit benötigen, fallen grundsätzlich nicht unter diese Regelung.

Für mehrere Standorte bzw. Filialen kann ein einziger DSB bestellt werden. Hierbei ist zu beachten, dass die Anzahl der Filialen nur so hoch sein darf, dass der DSB seine Aufgaben in jeder Filiale realistisch erfüllen kann.

Wer kann zum DSB benannt werden?

Der DSB kann sowohl ein Mitarbeiter des Betriebs (= interner DSB) oder ein außenstehender Dienstleister (= externer DSB) sein.
Unabhängig davon, ob es sich um einen internen oder externen DSB handelt, dürfen nur solche Personen bestellt werden, die

- fachliche Qualifikationen auf dem Gebiet des Datenschutzes besitzen (Datenschutzrecht und IT-Fachwissen) und

- bei der Aufgabenwahrnehmung in keinen Interessenskonflikt geraten können (Interessenskonflikte bestehen z.B. für Mitglieder der Geschäftsführung, Leiter der EDV oder der Personalabteilung, etc., da diese Personen für die Datenverarbeitung verantwortlich sind und sich als DSB selbst kontrollieren würden).

Welche Formalien sind zu beachten?

Eine bestimmte Form oder Dauer für die Bestellung sehen die gesetzlichen Regelungen nicht vor. Allein aus Nachweisgründen sollte die Bestellung in Textform erfolgen (siehe hierfür das Muster zur Bestellung eines DSB in **Anlage 7**).

Nach der Bestellung sind jedoch neue Informationspflichten zu beachten:

- Die Kontaktdaten des DSB (z.B. E-Mail-Adresse, Durchwahlnummer, etc.) sind zu veröffentlichen (z.B. auf der Webseite des Betriebs).

- Die Kontaktdaten des DSB sind der jeweiligen Landesdatenschutzbehörde zu melden.

Wichtig ist, dass nur über die Kontaktdaten zu informieren ist. Dies umfasst nicht zwingend den Namen des DSB.

Praxistipp: Um den Umstellungsaufwand bei Bestellung eines neuen DSB möglichst gering zu halten und eine erneute Veröffentlichung und Meldung an die Aufsichtsbehörde zu vermeiden, sollten allgemeine Kontaktadressen wie z.B. datenschutzbeauftragter@xy-betrieb.de oder datenschutz@xy-betrieb.de verwendet werden.

Wie ist die Stellung eines DSB?

Ein DSB ist bezüglich seiner Aufgabenerfüllung weisungsunabhängig. Er berichtet unmittelbar der Geschäftsführung und ist bei allen datenschutzrechtlichen Themen frühzeitig einzubinden.

Ein interner DSB darf wegen der Erfüllung seiner Aufgaben weder abberufen noch benachteiligt werden. Für seine zusätzliche Funktion als DSB sind ihm die notwendige Zeit und Unterstützung (z.B. Fortbildung, Ausstattung) zu geben. Ein interner DSB unterliegt zudem einem besonderen Kündigungsschutz: Das Arbeitsverhältnis darf während der Tätigkeit als

DSB und für ein Jahr danach nicht gekündigt werden, es sei denn, die Kündigung erfolgt aus wichtigem Grund.

Ein externer DSB gehört nicht dem Betrieb an. Infolgedessen gelten für ihn die besonderen Kündigungsschutzregeln nicht. Zudem kann der Dienstleistungsvertrag mit einem externen DSB grundsätzlich jederzeit gekündigt werden, soweit vertraglich nicht etwas anderes vereinbart wird.

Welche Aufgaben hat ein DSB zu erfüllen?

Einem DSB obliegen insbesondere folgende Aufgaben:

- Unterrichtung und Beratung sowohl der Geschäftsführung als auch der Mitarbeiter zu allen Belangen des Datenschutzes.
- Überwachung der Einhaltung der Datenschutzvorschriften.
- Sensibilisierung und Schulung der Mitarbeiter.
- Beratung und Überwachung der Durchführung von Datenschutz-Folgenabschätzungen (siehe hierzu Kapitel 6. Dokumentationspflichten).
- Zusammenarbeit mit der Landesdatenschutzaufsichtsbehörde.
- Ansprechpartner für externe und interne betroffene Personen zu allen Fragen zur Verarbeitung ihrer personenbezogenen Daten.

Welche Verantwortung trifft einen DSB?

Ein DSB ist für die ordnungsgemäße Erfüllung seiner gesetzlichen Aufgaben verantwortlich. Darüber hinausgehende Pflichten oder Haftungsrisiken bestehen nicht. Dies gilt insbesondere für die Einhaltung der datenschutzrechtlichen Vorschriften. Die Geschäftsführung bleibt trotz Benennung eines DSB für das rechtmäßige Handeln des Betriebs in Datenschutzangelegenheiten verantwortlich. Einen DSB trifft insoweit lediglich die Pflicht zur ordnungsgemäßen Beratung.

Welche Folgen drohen bei Nichtbestellung?

Die DSGVO sieht im Fall einer vorsätzlichen oder fahrlässigen Nichtbestellung erhebliche Bußgelder vor (bis zu 10 Mio. Euro oder zwei Prozent des weltweiten Jahresumsatzes).

8. Auftragsverarbeitung

Was ist eine Auftragsverarbeitung?

Eine Auftragsverarbeitung liegt vor, wenn ein Betrieb zwar personenbezogene Daten für seine Zwecke nutzt, die tatsächliche Verarbeitung und Aufbereitung dieser Daten aber nicht selbst durchführt, sondern von einem Dienstleister vornehmen lässt. Der Dienstleister verarbeitet die Daten für und im Auftrag des Betriebs. Dies ist z.B. bei Anbietern von Cloud-Lösungen der Fall, die auf ihren Servern Daten für den Betrieb speichern. Dasselbe gilt für Lohnbuchhaltungsanbieter, die für den Betrieb die Lohnbuchhaltung erstellen und dabei z.B. Mitarbeiterdaten verarbeiten.

Ist die Auftragsverarbeitung gesetzlich geregelt?

Die Auftragsverarbeitung ist hauptsächlich in Art. 28 der Datenschutz-Grundverordnung (DSGVO) geregelt. Darüber hinaus enthält die DSGVO vereinzelte Vorschriften, die jedoch für Handwerksbetriebe nicht einschlägig sind.

Das Gesetz bezeichnet den Dienstleister als „Auftragsverarbeiter“. Der beauftragende Betrieb wird „Verantwortlicher“ genannt, da er die Daten nutzt und damit trotz Einschaltung eines Dienstleisters auch für die Rechtmäßigkeit der Datenverarbeitung einstehen muss und verantwortlich bleibt. Deshalb haften bei Datenschutzverstößen Auftragsverarbeiter und Verantwortlicher gemeinsam.

Ist bei der Auftragsverarbeitung eine besondere Form zu beachten?

Art. 28 DSGVO schreibt keine besondere Form vor. In der Praxis ist es jedoch allein wegen der Dokumentation und aus Beweisgründen empfehlenswert, einen Vertrag in Textform zu schließen. So kann der Vertrag in elektronischen Formaten (z.B. PDF) oder schriftlich in Papierform geschlossen werden.

Welchen Inhalt muss eine Auftragsverarbeitung umfassen?

Art. 28 DSGVO normiert zahlreiche Mindestanforderung an den Inhalt einer Auftragsverarbeitung. Dies betrifft insbesondere folgende Aspekte:

- Gegenstand des Auftrags
- Dauer des Auftrags

- Zweck der Datenverarbeitung
- Art der zu verarbeitenden Daten
- Kategorien der betroffenen Personen
- Ergreifung der erforderlichen technischen und organisatorischen Maßnahmen
- Umfang der Weisungsbefugnisse
- Rückgabe von Datenträgern nach Beendigung des Auftrags

Muster einer Auftragsverarbeitung

Neben den vorgenannten Aspekten einer Auftragsverarbeitung sind weitere Punkte festzulegen. Es ist zu empfehlen, für die datenschutzrechtlichen Aspekte eines Auftragsverarbeitungsvertrags die Musterformulierungen in **Anlage 8** zu verwenden.

9. Rechtmäßige Datenverarbeitung von Beschäftigten

Gilt der Datenschutz auch in Beschäftigungsverhältnissen?

Ja. Für Beschäftigte gelten – wie für alle Personen – die Rechte der europäischen Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

Wer gilt als Beschäftigter?

Als Beschäftigte gelten neben Arbeitnehmern u.a. auch Bewerber, Auszubildende, Praktikanten und ausgeschiedene Arbeitnehmer.

Haben Beschäftigte besondere Datenschutzrechte?

Nein. Der Gesetzgeber geht zwar davon aus, dass Beschäftigte in einem gewissen Abhängigkeitsverhältnis zu ihrem Arbeitgeber stehen. Dennoch haben Beschäftigte keine Sonderrechte. Im Bundesdatenschutzgesetz werden lediglich zur Klarstellung bestimmte allgemeine Datenschutzrechte nochmals gesondert für Beschäftigte geregelt (§ 26 BDSG).

Dürfen Arbeitgeber die Daten ihrer Beschäftigten erheben und verarbeiten?

Ja. Arbeitgeber dürfen sämtliche personenbezogenen Daten ihrer Beschäftigten erheben, speichern und nutzen, wenn sie zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich sind (§ 26 Abs. 1 BDSG). Dies betrifft z.B.

- Stammdaten wie Name, Anschrift, Geburtsdatum, Geschlecht, Bankverbindung, Staatsangehörigkeit,
- steuer- und sozialversicherungsrelevante Daten wie Steueridentifikationsnummer, Steuerklasse, Familienstand und Angaben zur Konfession,
- Gesundheitsdaten,
- weitere spezifische Daten wie z.B. die regelmäßige Vorlage des Führerscheins.

Einwilligung von Arbeitnehmern

Neben den Daten, die zwingend erforderlich sind, um das Arbeitsverhältnis durchzuführen, haben Arbeitgeber regelmäßig ein Interesse an weiteren Daten ihrer Mitarbeiter. Dies gilt z.B. für die Veröffentlichung von Fotos der Mitarbeiter auf der Firmen-Website oder die Durchführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsvorsorge. Die hierfür benötigten Daten dürfen nicht ohne weiteres erhoben und genutzt werden. Arbeitgeber benötigen für die Verarbeitung dieser Daten eine vorherige Einwilligung der Beschäftigten. Ein Muster für die Einwilligung in die Veröffentlichung von Fotos auf der Firmen-Website liegt als **Anlage 9** bei.

Einwilligungen sind nur wirksam, wenn sie freiwillig erklärt werden (siehe hierzu Kapitel 2 „Anforderungen der datenschutzrechtlichen Einwilligung“). Da im Beschäftigungsverhältnis von einer gewissen Abhängigkeit des Arbeitnehmers ausgegangen wird, müssen Arbeitgeber in besonderer Weise darauf achten, dass ihre Beschäftigten frei von Zwang, Druck oder Beeinflussung entscheiden, ob sie die Einwilligung erteilen oder nicht.

Welche Pflichten haben Arbeitgeber?

Die Verarbeitung von Beschäftigtendaten bringt im Wesentlichen dieselben Pflichten mit sich, wie z.B. bei der Verarbeitung von Kundendaten. Insofern haben Arbeitgeber insbesondere die gesetzlich vorgeschriebenen Informations- und Dokumentationspflichten zu erfüllen.

Arbeitgeber sind in diesem Zusammenhang verpflichtet:

- Die Beschäftigten sind zu Beginn des Beschäftigungsverhältnisses einmalig über die Verarbeitung ihrer Daten zu informieren. Eine Musterinformation für Arbeitnehmer finden Sie in **Anlage 10.** Eine Musterinformation für Auszubildende, die einige weitere Informationen umfasst, ist als **Anlage 11** beigefügt.

- Die Datenverarbeitungsprozesse einmalig zu dokumentieren. In Handwerksbetrieben beschränken sich diese Prozesse i.d.R. auf die Verarbeitung von Beschäftigtendaten zum Zweck der Lohnabrechnung und der Personalführung. Für diese Verfahren finden Sie in der **Anlage 12 und 13** bereits vorausgefüllte Dokumentationsmuster, die Sie lediglich um Ihre Betriebsangaben wie Adresse und Betriebsinhaber ergänzen müssen.

- Zudem müssen Beschäftigte zu Beginn ihrer Tätigkeit einmalig darauf verpflichtet werden, dass sie im Rahmen ihrer Arbeit alle relevanten Datenschutzvorschriften beachten und sorgfältig mit personenbezogenen Daten umgehen. Eine Musterverpflichtungserklärung, die vom Beschäftigten zu unterzeichnen ist, finden Sie in **Anlage 14**.

Dürfen Beschäftigte mit Videokameras gefilmt werden?

Beim Einsatz von Videokameras im Betrieb ist zu beachten, welcher Bereich des Betriebsgeländes gefilmt wird.

In öffentlich zugänglichen Räumen (z.B. Parkplatz, Geschäfts-, Empfangs- und Verkaufsräumen) dürfen Videokameras eingesetzt werden, wenn es hierfür ein berechtigtes Interesse gibt (Art. 6 Abs. 1 f) DSGVO). Ein berechtigtes Interesse ist beispielsweise die Aufklärung von Diebstählen. Zu berücksichtigen ist dabei allerdings stets auch das Schutzinteresse der gefilmten Personen. Ist das Schutzinteresse höher zu bewerten, ist der Einsatz von Kameras unzulässig. Dies gilt u.a., wenn Beschäftigte dauerhaft gefilmt werden und damit eine Vollzeitüberwachung stattfindet. Die Kamera sollte in diesem Fall so ausgerichtet werden, dass sie den Beschäftigten nicht oder nur gelegentlich erfasst.

In nicht öffentlich zugänglichen Räumen (z.B. Materiallager, Büro, Werkstatt) sind Kameras grundsätzlich nicht erlaubt, wenn hierbei Beschäftigte gefilmt werden. Dies gilt selbst dann, wenn die Beschäftigten nur gelegentlich und nicht dauerhaft aufgenommen werden. Das Filmen von Beschäftigten ist in nicht öffentlich zugänglichen Räumen nur zulässig, wenn die Beschäftigten ausdrücklich eingewilligt haben. Die Einwilligung in eine dauerhafte Videoüberwachung ist allerdings unzulässig, da eine solche Erklärung ersichtlich nicht freiwillig wäre. Ein Muster für die Einwilligung in den Einsatz von Videokameras liegt als **Anlage 15** bei.

10. Videoüberwachung im Betrieb

Zulässigkeit der Videoüberwachung

Der Einsatz von Videokameras auf Betriebsgeländen und in Betriebsräumen ist inzwischen üblich. Die Zulässigkeit einer solchen Videoüberwachung richtet sich zum einen danach, ob der überwachte Bereich öffentlich zugänglich ist oder nicht. Zum anderen ist für die Zulässigkeit relevant, wer gefilmt wird. Bei Kunden, unbeteiligten Passanten und vor allem Beschäftigten des Betriebs ergeben sich unterschiedliche Auswirkungen auf die Zulässigkeit der Videoüberwachung.

Öffentlich zugängliche Räume

In öffentlich zugänglichen Räumen des Betriebs (z.B. Parkplatz, Geschäfts-, Empfangs- und Verkaufsräumen) dürfen Videokameras ohne Einwilligung der gefilmten Personen eingesetzt werden, wenn es hierfür ein berechtigtes Interesse gibt (Art. 6 Abs. 1 f) DSGVO). Ein berechtigtes Interesse ist beispielsweise die Aufklärung von Diebstählen oder Sachbeschädigungen. Zur Prävention von Straftaten sind Videokameras dagegen nicht geeignet. Auch wenn Videokameras in gewissem Maße eine abschreckende Wirkung zugesprochen wird, können sie die Durchführung einer Straftat nicht verhindern.

Das berechtigte Interesse des Betriebs an der Videoüberwachung ist stets mit dem Schutzinteresse der gefilmten Personen abzuwägen. Ist das Schutzinteresse der gefilmten Personen höher zu bewerten, ist der Einsatz von Kameras unzulässig. Hier ist zu unterscheiden, wer gefilmt wird.

➔ **Kunden** haben i.d.R. kein höheres Schutzinteresse, da sie freiwillig und in Kenntnis der Videoüberwachung das Betriebsgelände betreten.

➔ **Passanten**, die nicht das Betriebsgelände betreten, sondern auf öffentlichen Wegen an dem Betriebsgelände vorbeigehen oder sich dort aufhalten, haben ein höheres Schutzinteresse. Zudem besteht in diesen Fällen bereits kein berechtigtes Interesse des Betriebs an einer Videoüberwachung. Der Einsatz von Kameras darf sich grundsätzlich nur auf das Betriebsgelände und nicht darüber hinaus auf öffentliche Straßen, Wege und Plätze erstrecken. Kameras sind deshalb stets so auszurichten, dass sie ausschließlich das Betriebsgelände filmen. Ist dies wegen der örtlichen Gegebenheiten nicht möglich (z.B. Eingangsbereich an einer öffentlichen Straße), ist die Kamera so zu positionieren, dass sie möglichst wenig von der öffentlichen Straße erfasst.

➔ **Beschäftigte** haben ein höheres Schutzinteresse, wenn sie dauerhaft gefilmt werden und damit eine Vollzeitüberwachung stattfindet. Die Kamera sollte deshalb so ausgerichtet wer-

den, dass sie Beschäftigte entweder gar nicht oder nur gelegentlich erfasst. (Weitere Informationen zum Thema Datenschutz bei Beschäftigten gibt Kapitel 9.)

Nicht öffentlich zugängliche Räume

In Betriebsräumen, die nicht für Kunden und andere Personen, sondern nur für Beschäftigte des Betriebs zugänglich sind (z.B. Materiallager, Büro, Werkstatt), ist der Einsatz von Kameras grundsätzlich nicht erlaubt, wenn hierbei Beschäftigte gefilmt werden. Dies gilt selbst dann, wenn die Beschäftigten nur gelegentlich und nicht dauerhaft aufgenommen werden.

Das Filmen von Beschäftigten in nicht öffentlich zugänglichen Räumen ist nur dann zulässig, wenn hierdurch ein bestimmter, berechtigter Zweck (z.B. Aufklärung von Diebstählen oder Sachbeschädigungen) verfolgt wird und die Beschäftigten in die Videoüberwachung eingewilligt haben. Die Möglichkeit zur Einwilligung beschränkt sich jedoch auf eine gelegentliche Überwachung. Eine dauerhafte Videoüberwachung ist stets unzulässig.

Eine Einwilligung kann entweder von jedem betroffenen Beschäftigten einzeln oder über eine Betriebsvereinbarung erklärt werden. Ein Muster für die Einwilligung in den Einsatz von Videokameras liegt als **Anlage 15** bei. (Weitere Informationen zu den Anforderungen einer Einwilligung von Beschäftigten gibt Kapitel 9.)

Hinweis zur Videoüberwachung

Personen, die von einer Kamera gefilmt werden, müssen hierüber spätestens im Zeitpunkt der Videoüberwachung in Kenntnis gesetzt werden. Dies resultiert aus den Informationspflichten der Datenschutz-Grundverordnung (Art. 13 DSGVO) und ermöglicht den betroffenen Personen zu entscheiden, ob sie sich in dem überwachten Bereich aufhalten wollen oder nicht.

Die Datenschutzaufsichtsbehörden der Bundesländer empfehlen einen Aushang mit Piktogramm und Angabe verschiedener Informationen. Dieser oder ein inhaltlich vergleichbarer Aushang ist am Ort der Videoüberwachung an einer für die gefilmten Personen erkennbaren Stelle zu platzieren. Das Muster der Datenschutzaufsichtsbehörden ist als **Anlage 16** beigefügt und in verschiedenen Varianten (z.B. Metallschild oder Aufkleber) im Handel erhältlich.

Löschfristen

Für die Löschung von Videomaterial gilt derselbe Grundsatz wie für alle erhobenen personenbezogenen Daten (Art. 17 Abs. 1 a) DSGVO). Hiernach sind Videoaufnahmen zu lö-

schen, wenn sie zur Erreichung des Zwecks, für den sie aufgenommen wurden (i.d.R. die Aufklärung von Straftaten), nicht mehr notwendig sind.

Die Datenschutzaufsichtsbehörden erachten eine Speicherdauer von 48 Stunden grundsätzlich für ausreichend, um die Verfolgung von Straftaten zu ermöglichen. Die Speicherdauer bezieht sich jedoch auf das gesamte Videomaterial. Für die konkreten Sequenzen, auf denen die Straftat zu sehen ist, gilt die Frist von 48 Stunden nicht. Diese Sequenzen sind zu löschen, wenn sie zur Strafverfolgung tatsächlich nicht mehr benötigt werden. Die Frist von 48 Stunden soll sicherstellen, dass Videomaterial nicht pauschal gespeichert wird, obwohl hieraus ersichtlich keine weiteren Maßnahmen resultieren.

Sonderfälle

Von der oben beschriebenen Videoüberwachung gibt es gängige Sonderformen. Zum einen werden Videoaufnahmen häufig nicht gespeichert, sondern lediglich in Echtzeit auf einem Monitor angezeigt. Diese Videoüberwachung in Echtzeit ist unter denselben Voraussetzungen wie die Videoüberwachung mit Speicherung zulässig. Lediglich die Vorschriften zur Löschung des Videomaterials sind nicht zu beachten.

Zum anderen werden zu Abschreckungszwecken häufig Kameraattrappen bzw. nicht angeschlossene Kameras verwendet. Solche Attrappen erfüllen jedoch nur dann ihren Zweck, wenn sie für die vermeintlich gefilmten Personen „echt“ wirken. Für die betroffenen Personen und ihr daraus resultierendes Verhalten macht es somit keinen Unterschied, ob die Kamera filmt oder nicht. Deshalb dürfen auch solche Attrappen nur unter den Voraussetzungen einer tatsächlichen Videoüberwachung verwendet werden.

11. Löschkonzept für Daten

Wann sind Daten zu löschen?

Die Datenschutz-Grundverordnung (DSGVO) folgt einem praktikablen Grundsatz. Nach Art. 17 Abs. 1 DSGVO sind Daten stets dann zu löschen, wenn sie für den Zweck, zu dem sie erhoben wurden, nicht mehr erforderlich sind.

> **Beispiel:**
> Ein Verbraucher möchte Renovierungsarbeiten durchführen lassen und bittet einen Handwerker, zwecks Erstellung eines Kostenanschlags Aufmaß zu nehmen. Hierfür muss der Handwerker den Namen, die Wohnanschrift und gegebenenfalls weitere Kontaktdaten erheben. Kommt im Nachgang zum Kostenanschlag kein Vertrag zustande, benötigt der Handwerker die Daten des Verbrauchers nicht mehr.

Ob und wann die Aufbewahrung von Daten nicht mehr erforderlich ist, liegt grundsätzlich im Ermessen des Dateninhabers, also des Handwerksbetriebs, der die Daten erhoben hat. Allerdings haben sich in der Praxis gewisse Fristen etabliert, nach deren Ablauf in der Regel anzunehmen ist, dass eine weitere Aufbewahrung nicht mehr erforderlich ist. Diese ergeben sich meistens aus Verjährungsfristen, nach deren Ablauf ein Vorgang nicht mehr relevant ist. Siehe hierzu die tabellarische Übersicht der **Anlage 17**.

Aufbewahrungspflichten

Unabhängig davon, ob ein Handwerksbetrieb die erhobenen Daten noch oder nicht mehr benötigt, schreiben zahlreichliche gesetzliche Regelungen vor, dass bestimmte Daten mindestens für einen konkreten Zeitraum aufzubewahren sind. Solche Aufbewahrungspflichten gelten beispielsweise für steuerrelevante Daten wie Rechnungen oder Daten die Arbeitnehmer betreffen (z.B. Arbeitsverträge). Siehe für eine Übersicht der gesetzlichen Aufbewahrungspflichten die **Anlage 17**.

Während des gesetzlich vorgeschriebenen Aufbewahrungszeitraums dürfen die Daten nicht gelöscht werden. Nach Ablauf der gesetzlichen Frist dürfen die Daten gelöscht werden. Das bedeutet jedoch nicht, dass die Daten zwingend gelöscht werden müssen. Ob eine Pflicht zur Löschung besteht, ergibt sich zunächst aus dem allgemeinen Grundsatz der DSGVO (siehe oben). Hiernach sind die Daten nach Ablauf der gesetzlichen Aufbewahrungsfrist dann zu löschen, wenn sie nicht mehr für den Zweck, für den sie erhoben wurden, erforderlich sind.

Eine Pflicht zur Löschung kann zudem aus konkreten gesetzlichen Löschungspflichten folgen.

Gesetzliche Löschfristen

In vereinzelten Fällen schreiben gesetzliche Regelungen vor, wann bestimmte Daten zu löschen sind (für eine Übersicht gesetzlicher Löschfristen siehe die **Anlage 17**). Eine längere Aufbewahrung solcher Daten ist unzulässig.

Etwas anderes gilt nur dann, wenn die Daten zu einem anderen Zweck als zu dem, zu dem sie ursprünglich erhoben wurden, weiterhin benötigt werden. Eine solche Zweckänderung oder Zweckerweiterung ist jedoch an gesetzliche Zulässigkeitsvoraussetzungen gebunden (Art. 6 Abs. 4 DSGVO).

> **Beispiel:**
> Kundendaten werden nach Ablauf der Gewährleistungsfristen und der steuerrechtlichen Aufbewahrungspflichten – d.h. nach zehn Jahren – nicht mehr zur Abwicklung des Vertrags benötigt. Die Daten des Kunden können jedoch für die weitere Geschäftsbeziehung und zur Kundenbindung erforderlich sein. Für diese Zwecke dürfen die Daten in der Regel weiterhin aufbewahrt werden.

Was ist ein Löschkonzept?

Im Zusammenhang mit der Löschung von Daten wird häufig von einem Löschkonzept gesprochen. Damit ist gemeint, dass jeder Betrieb einen Überblick darüber haben sollte, welche Daten vorhanden/gespeichert sind und wann diese unter Beachtung der vorstehenden Regeln gelöscht werden.

Wie ist zu löschen?

Sind Daten weder weiterhin aufzubewahren noch archivwürdig, müssen sie gelöscht werden. Löschung bedeutet tatsächliche Vernichtung. Wurden Daten in Papierform aufbewahrt, ist das Papier zu schreddern, zu verbrennen oder auf sonstige Weise zu vernichten. Im Fall einer digitalen Speicherung sind die Daten unwiderruflich vom jeweiligen Datenträger (Festplatte, USB-Stick, etc.) zu löschen. Datenträger, die keine digitale Löschung ermöglichen – z.B. CDs – sind körperlich zu vernichten.

Für die ordnungsgemäße Löschung/Entsorgung werden in der Praxis häufig Dienstleister beauftragt. Die Löschung durch Dienstleister stellt eine Auftragsverarbeitung dar, die den Abschluss eines entsprechenden datenschutzrechtlichen Verarbeitungsvertrags erfordert. Weitere Informationen, Hinweise und Muster zur Auftragsdatenverarbeitung finden Sie im Praxis Datenschutz zur Auftragsverarbeitung.

Löschprotokoll

Wie bei allen Pflichten der DSGVO muss auch bei der Löschung von Daten nachgewiesen werden können, dass diese Pflicht ordnungsgemäß erfüllt wurde (Art. 5 Abs. 2 DSGVO). Diesbezüglich empfiehlt sich die Anfertigung eines Löschprotokolls. Dieses bedarf keiner besonderen Form. Es sollte jedoch selbst keine personenbezogenen Daten enthalten, sondern nur dokumentieren, dass eine Löschung vorgenommen wurde.

12. Datenschutz bei Betriebsnachfolge und Betriebsverkauf

Kundendaten sind datenschutzrelevant

Der Wert eines Betriebs bemisst sich neben Sachwerten, wie etwa Maschinen, Werkzeugen und Immobilien, auch nach der Größe des Kundenstamms. Gerade im Handwerk sind langfristige Kundenbindungen üblich. Käufer eines Handwerksbetriebs beabsichtigen meist, bestehende Kundenbeziehungen fortzuführen und haben deshalb Interesse an den Kundendaten.

Kundendaten unterstehen jedoch dem Schutz der Datenschutz-Grundverordnung (DSGVO), die bei einem Unternehmensverkauf zu beachten ist. Dies gilt auch für die Daten der Beschäftigten. So dürfen Informationen etwa über die Mitarbeiter- und Altersstruktur im Vorfeld der Betriebsübernahme nur mit Einwilligung der Beschäftigten erteilt werden.

Welche Anforderungen für eine zulässige Datenübertragung von Kundendaten gelten, richtet sich danach, ob es sich bei dem Betrieb um eine GmbH oder um ein inhabergeführtes Unternehmen bzw. eine Personengesellschaft handelt.

Datenverkauf bei GmbHs

Wird eine GmbH verkauft, so wechseln lediglich die Gesellschafter. Die GmbH als eigenständige Rechtsperson bleibt unverändert bestehen. Dementsprechend verbleiben auch die Kundendaten bei der GmbH. Es findet somit keine Datenübertragung von den bisherigen auf die neuen Gesellschafter statt. Deshalb sind beim Verkauf einer GmbH diesbezüglich in der Regel keine gesonderten Datenschutzvorschriften zu beachten. Das gleiche gilt für andere Kapitalgesellschaftsformen, wie z.B. die Aktiengesellschaft (AG).

Datenverkäufe bei inhabergeführten Betrieben und Personengesellschaften

Anders als bei Kapitalgesellschaften gehen beim Verkauf inhabergeführter Betriebe oder Personengesellschaften die Vermögens- und Sachwerte vom Verkäufer auf den Käufer über. Das gilt auch für Kundendaten. Hierbei findet die DSGVO Anwendung. Kundendaten dürfen hiernach ohne Einwilligung des Kunden übertragen werden (Art. 6 Abs. 1 f) DSGVO). Den Kunden steht aber ein Widerspruchsrecht zu. Deshalb muss der alte Betriebsinhaber die Kunden im Vorlauf zum Betriebsverkauf über die beabsichtigte Datenübertragung informieren und ihnen die Möglichkeit zum Widerspruch einräumen. Ein Muster liegt als **Anlage 18** bei.

Eine Besonderheit besteht für Betriebe der Gesundheitshandwerke. Da es sich bei den gespeicherten Gesundheitsdaten der Kunden um besonders schutzwürdige Daten handelt (Art.

7 DSGVO), ist die Einwilligung der Kunden zwingend erforderlich. Eine Mustereinwilligung liegt als **Anlage 19** bei.

Wettbewerbsrecht beachten

Obwohl der neue Betriebsinhaber die Kundendaten auf datenschutzrechtlich zulässige Weise erworben hat, ist bei der Verwendung von bestimmten Kommunikationsdaten (Telefonnummer, E-Mail-Adresse, Fax) darauf zu achten, dass diese nur genutzt werden dürfen, wenn der Kunde seine Zustimmung erteilt. Diese Anforderung resultiert aus dem Wettbewerbsrecht (§ 7 Gesetz gegen den unlauteren Wettbewerb – UWG).

Eine postalische Kontaktaufnahme ist hiervon nicht erfasst und kann ohne weitere Voraussetzungen erfolgen. Ein Muster liegt als **Anlage 20** bei.

13. Datenschutz bei Betrieben der Gesundheitshandwerke

Warum gelten für Gesundheitshandwerke zum Teil besondere Vorschriften?

Informationen über die Gesundheit einer Person gelten – wie nach bisherigem Recht auch – als besonders sensible Daten und unterstehen einem strengen gesetzlichen Schutz. Da Betriebe der Gesundheitshandwerke Gesundheitsdaten ihrer Kunden erheben, speichern und nutzen (z.B. Dioptrinzahl, Hörfähigkeit, etc.), müssen sie die besonderen Vorschriften beachten.

Dürfen Gesundheitshandwerker die Gesundheitsdaten ihrer Kunden nur mit deren Einwilligung erheben und nutzen?

Nein. Zwar ordnet die Datenschutz-Grund-verordnung an, dass für die Erhebung und Verarbeitung von Gesundheitsdaten grundsätzlich eine Einwilligung erforderlich ist. Das Bundesdatenschutzgesetz macht von dieser Regel jedoch eine entscheidende Ausnahme. So sind alle Berufsgruppen, die einer Geheimhaltungspflicht unterstehen, von der Pflicht einer Einwilligung befreit.

Neben gesetzlichen Geheimhaltungspflichten sind hiervon auch solche Geheimhaltungspflichten umfasst, die in der jeweiligen Berufsordnung vorgeschrieben sind. Dies hat das Bundesministerium des Innern ausdrücklich bestätigt.

Die Berufsordnungen der Gesundheitshandwerke umfassen solche Geheimhaltungspflichten. Deshalb müssen Gesundheitshandwerker keine Einwilligung ihrer Kunden einholen, wenn sie die Gesundheitsdaten erheben und zur Auftragserfüllung verarbeiten.

Müssen Gesundheitshandwerker einen Datenschutzbeauftragten bestellen?

Ein Datenschutzbeauftragter muss bestellt werden, wenn ein Betrieb Gesundheitsdaten umfangreich verarbeitet (§ 38 BDSG, Art. 35 DSGVO). Zwar verarbeiten Gesundheitshandwerker Gesundheitsdaten, jedoch geschieht dies nicht in umfangreicher Weise. So wird lediglich ein Gesundheitsdatum pro Kunde erhoben und verarbeitet. Im Vergleich zu Krankenhäusern oder großen Arztpraxen, die sowohl zahlreiche unterschiedliche Gesundheitsdaten als auch eine weitaus höhere Anzahl an Patienten betreuen, wird der geringe Umfang deutlich. Dies wird auch von der Datenaufsichtsbehörde des Landes Bayern bestätigt.

Für Gesundheitshandwerker gelten somit i.d.R. dieselben Regelungen wie für andere Handwerksbetriebe. Sie müssen einen Datenschutzbeauftragten bestellen, wenn im Betrieb mindestens zehn Mitarbeiter (ab voraussichtlich Oktober 2019 zwanzig Mitarbeiter) ständig mit

der automatisierten Verarbeitung von Daten befasst sind (§ 38 BDSG). Als „ständig befasst“ gelten nur solche Mitarbeiter, deren alltägliche Kerntätigkeit die Verarbeitung von Daten ist. Dies ist z.B. bei Mitarbeitern der Lohnbuchhaltung oder der Personalabteilung der Fall. Mitarbeiter, die lediglich die Daten zur Ausübung ihrer handwerklichen Tätigkeit benötigen, fallen grundsätzlich nicht unter diese Regelung.

ANLAGEN

Anlage 1

Anforderungen der datenschutzrechtlichen Einwilligung

Muster

Einwilligungserklärung

In unserem Werbenewsletter informiert die **Mustermannbetrieb GmbH** ihre Kunden postalisch oder per E-Mail über Aktionsrabatte, aktuelle Leistungen und Neuigkeiten. Dies ist ein kostenloser Service für Sie.

☐ **Ja, ich/wir bin/sind damit einverstanden**, dass meine/unsere Kontaktdaten

(Name, Adresse, Faxnummer und E-Mail-Adresse) zum Zweck der Produktwerbung und Informationen zum Leistungsspektrum des Betriebs gespeichert und zur Kontaktaufnahme genutzt werden.

Mir/uns ist dabei klar, dass diese Einwilligungen freiwillig und jederzeit widerruflich sind. Der Widerruf ist

per E-Mail zu richten an: info@mustermannbetrieb.de

oder postalisch an: Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt

Nach Erhalt des Widerrufs werden wir die betreffenden Daten nicht mehr nutzen und verarbeiten bzw. löschen.

_____

Ort, Datum, Unterschrift

Die Datenverarbeitung ist für die Zusendung der Produktwerbung per E-Mail erforderlich und beruht auf Artikel 6 Abs. 1 a) DSGVO. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Sie können unseren Datenschutzbeauftragten unter datenschutz@mustermannbetrieb.de oder unter Datenschutzbeauftragter c/o Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, erreichen.

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 2

Informationspflichten bei Erhebung personenbezogener Daten

Muster

Information bei Erhebung von Daten beim Betroffenen

Informationen zur Datenerhebung gemäß Artikel 13 DSGVO

Die Musterbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, Geschäftsführerin Frau Musterfrau, erhebt Ihre Daten zum Zweck der Vertragsdurchführung, zur Erfüllung ihrer vertraglichen und vorvertraglichen Pflichten sowie zur Direktwerbung.

Die Datenerhebung und Datenverarbeitung ist für die Durchführung des Vertrags und zur Direktwerbung erforderlich und beruht auf Artikel 6 Abs. 1 b), f) DSGVO. Mit der Direktwerbung wollen wir Sie über aktuelle Leistungen und Neuigkeiten unseres Betriebs informieren. Eine Weitergabe der Daten an Dritte findet grundsätzlich nicht statt. Gegebenenfalls werden die Daten zwecks Erfüllung steuerrechtlicher Pflichten an einen Steuerberater und bei ausstehenden Zahlungen zwecks Inkassomaßnahmen an Dienstleister weitergegeben. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Direktwerbung jederzeit zu widersprechen. Zudem sind Sie berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Sie können unseren Datenschutzbeauftragten unter datenschutz@musterbetrieb.de oder unter Datenschutzbeauftragter c/o Musterbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, erreichen.

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 2 A

Informationspflicht bei Erhebung personenbezogener Daten auf Webseiten

Beispielsformulierungen zur Ergänzung des Datenschutzhinweises

Die Datenschutzerklärung auf Webseiten richtet sich danach, ob und inwieweit personenbezogene Daten auf der Webseite erhoben werden. Dies kann z.B. durch ein Tracking-Tool, Kontaktformulare oder Bestellungen von Newslettern der Fall sein und muss in jedem Einzelfall individuell angefertigt werden. Für typische Verarbeitungssituationen können Sie folgende Beispielformulierungen verwenden.

Kontaktformular

Wir erheben Ihre Daten zum Zweck der Durchführung Ihrer Kontaktanfrage. Die Datenverarbeitung beruht auf Artikel 6 Abs. 1 f) DSGVO. Unser berechtigtes Interesse ist, Ihre Anfrage zu beantworten. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind. Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Kontaktaufnahme jederzeit zu widersprechen.

Newsletter

Wir erheben Ihre Daten zum Zweck der Zusendung des von Ihnen gewünschten Informationsmaterials. Die Datenverarbeitung beruht auf Ihrer Einwilligung gemäß Artikel 6 Abs. 1 a) DSGVO. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind. Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Zusendung von Informationsmaterialien jederzeit zu widersprechen.

Registrierung im Mitgliederbereich

Wir erheben Ihre Daten zum Zweck der Durchführung Ihrer Anmeldung für den Mitgliederbereich von www…..de. Die Datenverarbeitung beruht auf Artikel 6 Abs. 1 f) DSGVO. Wir verfolgen das Interesse, sicherzustellen, dass nur Mitglieder Zugriff auf den Mitgliedern vorbehaltenen Informationen erhalten. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind. Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Registrierung jederzeit zu widersprechen.

Ihre Rechte

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Datenschutzbeauftragter

Wenn ein Datenschutzbeauftragter benannt werden muss, müssen dessen Kontaktdaten ebenfalls auf der Webseite genannt werden.

Anlage 3

Die Erteilung von Auskünften

MUSTER

Auskunftserteilung eines Handwerksbetriebs an einen Kunden

Herrn/Frau
Michael(a) Muster
Mustergasse 1
33333 Musterstadt

Sehr geehrte/r Frau/Herr _____,

Sie haben uns um Auskunft darüber gebeten, welche Daten wir zu Ihrer Person gespeichert haben. Sie sind bei uns als ……(z.B. Kunde/Interessent) erfasst.

Zur Datenverarbeitung durch unser Unternehmen teilen wir Ihnen mit, dass die Datenerhebung zur Kommunikation mit Ihnen, Abgabe von Angeboten, Abrechnung von Leistungen oder zur Erfüllung von Verträgen erfolgt. Diese Daten haben Sie uns mitgeteilt. Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung erforderlich sind. Sofern Daten hiervon nicht erfasst sind, werden sie gelöscht, sobald sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden. Die Daten werden nicht an Dritte weitergeben. Die über Sie gespeicherten Daten entnehmen Sie bitte der beigefügten Tabelle.

Wir hoffen, dass wir mit den vorstehenden Ausführungen Ihre Fragen hinreichend beantworten konnten. Informieren Sie uns bitte, falls Daten unrichtig sind.

Sie haben das Recht, sich bei der für uns zuständigen Datenschutzaufsichtsbehörde ……..(Name, Adresse, E-Mail) zu beschweren, falls Sie der Meinung sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Für weitere Auskünfte stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

Firma ……..

Anlage

Kunde	
Familienname	
Vorname	
Geburtsname	
Geschlecht	
Geburtsdatum	
Staatsangehörigkeit	
Straße	
PLZ	
Wohnort	
UstID	
Kommunikationsdaten	
Telefon	
Handy	
E-Mail	
Bankverbindung	
Bankname	
IBAN-Nummer	
BIC	
Kundenspezifische Daten	
z.B. Wartungsverträge …	

Anlage 4

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

Angaben zum Verantwortlichen, Art. 30 Abs. 1 a) DSGVO

1. Verantwortlicher (= Firma/Legaleinheit)

2. Gesetzlicher Vertreter (= Geschäftsführung)

3. Datenschutzbeauftragter

Name:

Anschrift:

E-Mail:

Tel.:

4. Zuständige Aufsichtsbehörde

Landesbeauftragter für Datenschutz und Informationsfreiheit Bundesland XY

Verpflichtende Meldung des/der Datenschutzbeauftragten bereits erfolgt:

☐ Ja

☐ Nein

5. Regelungen zur Datensicherheit

IT-Sicherheitskonzept

[Verweis auf übergreifende IT-Sicherheitskonzepte, die grundsätzlich für alle Verarbeitungstätigkeiten gelten]

6. Sachverhalte zu Drittstaatenübermittlungen

Erläuterungen zum Hauptblatt

Nr. 1	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO) Angaben: Name/Firma, ladungsfähige Anschrift
Nr. 2	Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter Angaben: Namen der geschäftsführenden Personen *Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.*
Nr. 3	Vom Verantwortlichen bestellter Datenschutzbeauftragter (sofern ein Datenschutzbeauftragter bestellt wurde) Angaben: Name, Kontaktdaten
Nr. 4	Die Meldung der Kontakt-Informationen des Datenschutzbeauftragten (Funktions-)E-Mail-Adresse und Telefonnummer sind Pflichtangaben
Nr. 5	Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grds. alle Verarbeitungen* betreffen) Der Verweis auf übergreifende Regelungen an dieser Stelle entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten. Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines ISMS nach ISO27001.
Nr. 6	Ein Verweis zur Regelungen zur Drittstaatenübermittlung ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR.

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis Nr. _____

☐ Ersterstellung

☐ Änderung eines bestehenden Verzeichnisses

Erstellungsdatum:

Bezeichnung der Verarbeitungstätigkeit:

I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO

1. Verantwortlicher Fachbereich/verantwortliche Führungskraft

2. Bei gemeinsamer Verantwortlichkeit:
Name und Kontaktdaten des Leiters/der Leiter oder des/der weiteren Verantwortlichen

II. Angaben zur Verarbeitungstätigkeit

3. Risikobewertung
Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?

☐ Nein

☐ Ja

Wenn ja, dann Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Art. 35 DSG-VO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO	
6.1. Betroffene Personengruppen	**6.2. Kategorien personenbezogener Daten**

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO	
7.1. Interne Empfänger	
7.2. Externe Empfänger	
7.3. Vertragliche Dienstleister (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen)	

8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 e) DSGVO

Übermittlung

☐ Nein

☐ Ja

Wenn ja, dann: Name des Drittlandes / der internationalen Organisation

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO
10.1. Art der eingesetzten Datenverarbeitungsanlagen und Software (optional)
10.2. Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

----- Optionale Angaben ----

Weitere Dokumentationen zur Verarbeitungstätigkeit

----- Ende Optionale Angaben----

Erläuterungen zum Verarbeitungsverzeichnis

Nr. 1	Eindeutige Bezeichnung der dokumentierten Verarbeitung/ Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: - Allgemeine Kundenverwaltung - Customer-Relationship-Management (CRM)
Nr. 1	Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*)
Nr. 2	Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten des/der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 a) DSGVO, Art. 26 Abs. 1 DSGVO)
Nr. 3	Es ist zu bewerten, ob die Datenverarbeitung ein hohes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind. Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten) umfangreich verarbeitet werden.
Nr. 4	Beispiele: - Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“ - Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“ Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können. Die erforderliche Detailtiefe hängt von der Geschäftstätigkeit des Verantwortlichen ab. Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen wie z.B. zur Personalführung/-einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung oder als eigene Verarbeitung beschrieben sein.
Nr. 5	Die Nennung der einschlägigen Rechtsgrundlage ist für Rechenschaftspflichten und die Gewährleistung von Transparenzpflichten ggü. den betroffenen Personen notwendig. Die Rechtsgrundlage können z.B. eine gesetzliche Vorschrift oder eine Einwilligung durch den Betroffenen sein.
Nr. 6	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO
Nr. 6.1	Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht.
Nr. 6.2	Den einzelnen Personengruppen sind die jeweils auf sie bezogenen ver-

	wendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern "Datenbezeichnungen"/Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Nicht ausreichend sind etwa Angaben wie „Kundendaten“ oder Ähnliches. Beispiele: - Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließlich Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung - Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.
Nr. 7	Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
Nr. 8	Drittländer sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, der EU. Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren, Art. 49 Abs. 1. UAbs. 2 DSGVO.
Nr. 9	Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.
Nr. 10	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO.
Nr. 10.1	Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.
Nr. 10.2	Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend. Insbesondere sind hier Abweichungen zu einem übergreifenden Sicherheitskonzept (**siehe Hauptblatt Nr. 5**) zu dokumentieren. Wenn eine Datenschutz-Folgenabschätzung für die Verarbeitung hohe Risiken ausweist, so sind die zur Bewältigung dieser Risiken getroffenen Sicherheitsvorkehrungen für die Verarbeitung in der Datenschutz-Folgenabschätzung zu dokumentieren, Art. 35 Abs. 7 d) DSGVO. Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe (siehe unten).

Optional	Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B. • *Angaben zur Zusammenstellung der Informationspflichten (insbes. Art. 13,14 DSGVO)* • *Verträge mit Dienstleistern (Art. 28 DSGVO)* • *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO)* • *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen* • *durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)*

Anlage 5

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

Angaben zum Verantwortlichen, Art. 30 Abs. 1 a) DSGVO

1. Verantwortlicher (=Firma/Legaleinheit)
Mustermann GmbH, Musterstraße 17-21, 12345 Musterstadt

2. Gesetzlicher Vertreter (= Geschäftsführung/ Betriebsinhaber)
Herr Otto Mustermann, Musterstraße 17-21, 12345 Musterstadt

3. Datenschutzbeauftragter

Name: Frau Anja Mustermann

Anschrift: Musterstraße 17-21,12345 Musterstadt

E-Mail: datenschutzbeauftragter@mustermann-gmbh.de

Tel.: 01234/ 123456-34

4. Zuständige Aufsichtsbehörde
Landesbeauftragter für Datenschutz und Informationsfreiheit NRW

Verpflichtende Meldung des/der Datenschutzbeauftragten bereits erfolgt:

☒ Ja
☐ Nein

5. Regelungen zur Datensicherheit
IT-Sicherheitskonzept der HWK Musterstadt

6. Sachverhalte zu Drittstaatenübermittlungen
Findet nicht statt.

Erläuterungen zum Hauptblatt

Nr. 1	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO) Angaben: Name/Firma, ladungsfähige Anschrift
Nr. 2	Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter Angaben: Namen der geschäftsführenden Personen *Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.*
Nr. 3	Vom Verantwortlichen bestellter Datenschutzbeauftragter (sofern ein Datenschutzbeauftragter bestellt wurde) Angaben: Name, Kontaktdaten
Nr. 4	Die Meldung der Kontakt-Informationen des Datenschutzbeauftragten (Funktions-)E-Mail-Adresse und Telefonnummer sind Pflichtangaben.
Nr. 5	Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grds. alle Verarbeitungen* betreffen) Der Verweis auf übergreifende Regelungen an dieser Stelle entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten. Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines ISMS nach ISO27001.
Nr. 6	Ein Verweis zur Regelungen zur Drittstaatenübermittlung ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR.

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis Nr. 1

☒ Ersterstellung

☐ Änderung eines bestehenden Verzeichnisses

Erstellungsdatum: 21.8.2017

Bezeichnung der Verarbeitungstätigkeit: Erstellung und Führung der Kundendatei

I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO

1. Verantwortlicher Fachbereich/verantwortliche Führungskraft
Herr Mustermann

2. Bei gemeinsamer Verantwortlichkeit:
Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen

II. Angaben zur Verarbeitungstätigkeit

3. Risikobewertung
Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?

☒ Nein

☐ Ja

Wenn ja, dann Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Art. 35 DSG-VO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit
Organisation von Geschäftskontakten und Bestandskunden.
Durchführung von Verträgen.
Nutzung zur Direktwerbung.

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit
Art. 6 Abs. 1 b DSGVO

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO	
6.1. Betroffene Personengruppen	**6.2. Kategorien personenbezogener Daten**
Kunden, Geschäftspartner	Name, Vorname, Adressdaten, (elektronische) Kontaktdaten, ggfs. Firma oder Etablissementbezeichnung, Datum des Auftrags, Gegenstand des Auftrags

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO	
7.1. Interne Empfänger	Vertriebsmitarbeiter, Mitarbeiter im Außendienst
7.2. Externe Empfänger	--------
7.3. Vertragliche Dienstleister (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen)	--------

8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 e) DSGVO

Übermittlung

☒ Nein

☐ Ja

Wenn ja, dann: Name des Drittlandes / der internationalen Organisation (DSGVO)

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO

Die Datenwerden gelöscht, wenn sie für die Erfüllung des Zweck (siehe Nr. 4) nicht mehr erforderlich sind.

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

Siehe betriebsinternes IT-Sicherheitskonzept

10.1 Art der eingesetzten DV-Anlagen und Software (optional)

(Siehe betriebsinternes IT-Sicherheitskonzept)

10.2 Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

(Siehe betriebsinternes IT-Sicherheitskonzept)

----- *Optionale Angaben* ----

Weitere Dokumentationen zur Verarbeitungstätigkeit

----- *Ende Optionale Angaben*----

Erläuterungen zum Verarbeitungsverzeichnis

Nr. 1	Eindeutige Bezeichnung der dokumentierten Verarbeitung/ Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: - Allgemeine Kundenverwaltung - Customer-Relationship-Management (CRM)
Nr. 1	Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*)
Nr. 2	Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten des/der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 a) DSGVO, Art. 26 Abs. 1 DSGVO)
Nr. 3	Es ist zu bewerten, ob die Datenverarbeitung ein hohes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind. Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten) umfangreich verarbeitet werden.
Nr. 4	Beispiele: - Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“ - Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“ Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können. Die erforderliche Detailtiefe hängt von der Geschäftstätigkeit des Verantwortlichen ab. Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen wie z.B. zur Personalführung/-einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung oder als eigene Verarbeitung beschrieben sein.
Nr. 5	Die Nennung der einschlägigen Rechtsgrundlage ist für Rechenschaftspflichten und die Gewährleistung von Transparenzpflichten ggü. den betroffenen Personen notwendig. Die Rechtsgrundlage können z.B. eine gesetzliche Vorschrift oder eine Einwilligung durch den Betroffenen sein.
Nr. 6	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO
Nr. 6.1	Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht.
Nr. 6.2	Den einzelnen Personengruppen sind die jeweils auf sie bezogenen ver-

	wendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern "Datenbezeichnungen"/Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Nicht ausreichend sind etwa Angaben wie „Kundendaten“ oder Ähnliches. Beispiele: - Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließlich Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung - Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.
Nr. 7	Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
Nr. 8	Drittländer sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, der EU. Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren, Art. 49 Abs. 1. UAbs. 2 DSGVO.
Nr. 9	Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.
Nr. 10	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO.
Nr. 10.1	Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.
Nr. 10.2	Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend. Insbesondere sind hier Abweichungen zu einem übergreifenden Sicherheitskonzept (**siehe Hauptblatt Nr. 5**) zu dokumentieren. Wenn eine Datenschutz-Folgenabschätzung für die Verarbeitung hohe Risiken ausweist, so sind die zur Bewältigung dieser Risiken getroffenen Sicherheitsvorkehrungen für die Verarbeitung in der Datenschutz-Folgenabschätzung zu dokumentieren, Art. 35 Abs. 7 d) DSGVO. Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe (siehe unten).

Optional	Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B. • *Angaben zur Zusammenstellung der Informationspflichten (insbes. Art. 13,14 DSGVO)* • *Verträge mit Dienstleistern (Art. 28 DSGVO)* • *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO)* • *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen* • *durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)*

Anlage 6

Technische und organisatorische Maßnahmen

1. Organisatorische Maßnahmen

☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?
☐ Nein
☐ Ja
Name: ……..
Funktion: ……
E-Mail: ……
Telefon: ……..
☐ Mitarbeiter wurden nachweislich über Datenschutzrecht und Datensicherheit geschult.
☐ Alle Mitarbeiter sind nachweislich auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.
☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z.B. technisch unterstützt oder durch Externe).
☐ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden.
☐ Ein Datenschutzkonzept ist vorhanden.
☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am _____und Bestätigung s. Anlage ____).
☐ Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am _____und Bestätigung s. Anlage ____).

2. Vertraulichkeit

a) Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle
Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
☐ Alarmanlage
☐ Automatisches Zutrittskontrollsystem, Ausweisleser
☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
☐ Sicherheitsschlösser
☐ Chipkarten-/Transponder-Schließsystem
☐ Biometrie (Fingerabdrücke o. ä.)
☐ Manuelles Schließsystem
☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
☐ Magnetschleusen
☐ Werkschutz/Pförtner
☐ Empfang mit Anmeldung

- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Lichtschranke/Bewegungsmelder
- ☐ Feuerfeste Türen
- ☐ Absicherung von Gebäudeschächten
- ☐ Fenstervergitterung
- ☐ Panzerglas
- ☐ Videoüberwachung der Zugänge

b) *Zugangs- und Benutzerkontrolle*

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☐ Passwortvergabe
  Länge des Passworts: … Zeichen
  Wechselfristen … Wochen/Monate
  Anzahl der Fehleingaben …
- ☐ Chipkarte mit PIN/Passwort
- ☐ Authentifikation mit Benutzername/Passwort
- ☐ Biometrisches Merkmal mit PIN/Passwort
- ☐ Einsatz von VPN-Technologie
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von mobilen Datenträgern

c) *Zugriffskontrolle*

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☐ Schriftliches Berechtigungskonzept vorhanden
- ☐ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- ☐ Verwaltung der Rechte durch System-Administrator
- ☐ Anzahl der Administratoren auf das "Notwendigste" reduziert
- ☐ Gesicherte Nutzung von USB-Schnittstellen
- ☐ Installierung von Virenschutzprogrammen und anderer Schutzsoftware
- ☐ Automatische Sperrung des Arbeitsplatzes
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Die Protokolle werden ausgewertet, zeitlicher Abstand: ….
- ☐ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
- ☐ Verschlüsselung von Datenträgern
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Ordnungsgemäße Vernichtung von Datenträgern
- ☐ Löschungskonzept für Daten
- ☐ Protokollierung der Vernichtung

d) Transport- und Übertragungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Protokollierung von Übermittlungen
- ☐ Erstellen einer Übersicht von Datenträgern, Aus- und Eingang
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☐ Sicherung von Datenträgertransporten (verschließbarer Transportbehälter), auch für Papier

e) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☐ Vorhandene Vereinbarungen zur Auftragsverarbeitung
- ☐ Kontrolle der Vertragsausführung
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Regelung zu Wartungen (speziell Fernwartung)

3. Integrität

a) Eingabekontrolle/Verarbeitungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Protokollauswertungsroutinen/-systeme vorhanden
- ☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

b) Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- ☐ Führung eines Verarbeitungsverzeichnisses
- ☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
- ☐ Zulässigkeit eines Datentransfers in Drittländer ist gegeben

4. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können.

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Überspannungsschutz
- ☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Virenschutzsystem
- ☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
- ☐ Konzept für Katastrophenfall vorhanden

5. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Festlegung Technologie von Datenbankrechten
- ☐ Trennung von Daten verschiedener Auftraggeber

Anlage 7

Der betriebliche Datenschutzbeauftragte (DSB)

MUSTER

Benennung eines/r betrieblichen Datenschutzbeauftragten

Herrn/Frau
Michael(a) Muster
Mustergasse 1
33333 Musterstadt

Sehr geehrte/r Frau/Herr _____,

ich/wir benennen Sie mit sofortiger Wirkung zur/m Datenschutzbeauftragten gemäß Artikel 37 Abs. 1 b) und c) EU-Datenschutzgrundverordnung (DSGVO) in Verbindung mit § 38 Bundesdatenschutzgesetz (BDSG). In Ihrer Funktion als Datenschutzbeauftragte/r sind Sie der Geschäftsleitung unmittelbar unterstellt.

Zuständiges Mitglied der Geschäftsleitung ist

_____

Ihre Aufgaben als Datenschutzbeauftragte/r ergeben sich aus den Artikeln 37 bis 39 DSGVO sowie § 38 BDSG. In Anwendung Ihrer Fachkunde auf dem Gebiet des Datenschutzes sind Sie weisungsfrei. Bei der Erfüllung Ihrer Aufgaben sind Sie an die Wahrung der Geheimhaltung und der Vertraulichkeit gebunden. Über Ihre Tätigkeit werden Sie der Geschäftsleitung laufend Bericht erstatten.

Erforderliche Organisationsanweisungen schlagen Sie der Geschäftsleitung vor.

_____ _____
Ort, Datum Unterschrift Geschäftsleitung

Mit der Benennung bin ich einverstanden

_____
Unterschrift, Datenschutzbeauftragte/r

Anlage 8

Auftragsverarbeitung

Musterformulierungen

1. Gegenstand und Dauer des Auftrags

➔ Der Gegenstand und die Dauer des Auftrags müssen individuell mit dem Auftragsverarbeiter verhandelt und festgelegt werden.

➔ Musterformulierungen sind wegen der Individualität der Vereinbarungen nicht möglich.

2. Umfang, Art und Zweck der Datenverarbeitung

Formulierungsvorschlag:

„Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im sachlichen und zeitlichen Rahmen dieses Auftrages sowie nach Weisung des Auftraggebers. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

Die Verarbeitung der Daten auch durch Unterauftragnehmer findet

☐ ausschließlich im Gebiet der Bundesrepublik Deutschland,

☐ in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum,

☐ in einem Drittstaat (Nennung des Drittstaats _____)

statt. In letzterem Fall weist der Auftragnehmer für die Rechtmäßigkeit entsprechende vertragliche oder sonstige, der DSGVO entsprechenden Rechtsgrundlagen nach.“

3. Technische und organisatorische Maßnahmen

Formulierungsvorschlag:

„Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den gesetzlichen Anforderungen genügen. Hierbei sind die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Die technisch-organisatorischen Maßnahmen des Auftragnehmers sind gesondert zu diesem Vertrag festzulegen und sind Bestandteil des Vertrags.

Der Auftragnehmer gewährleistet ein Verfahren zur Überprüfung der technischen und organisatorischen Maßnahmen. Er ist verpflichtet, die technischen und organisatorischen Maßnahmen an den Stand der Technik anzupassen, soweit dies erforderlich und wirtschaftlich zumutbar ist. Der Auftraggeber ist über wesentliche Änderungen vorab zu informieren. Die Änderungen sind schriftlich niederzulegen und werden Vertragsbestandteil. Vorschläge des Auftraggebers für Änderungen hat der Auftragnehmer zu prüfen. Der Auftraggeber ist über das Ergebnis zu informieren.

Beauftragt der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten einen Unterauftragnehmer, stellt er sicher, dass die erforderlichen technischen und organisatorischen Maßnahmen vom Unterauftragnehmer getroffen werden und dem Stand der Technik entsprechen."

4. Berichtigung, Sperrung und Löschung von Daten, Auskunft über Daten

Formulierungsvorschlag:

„Der Auftragnehmer hat die Daten nach Weisung des Auftraggebers zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten wendet, leitet der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiter. Das gleiche gilt für Auskunftsersuche."

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Formulierungsvorschlag:

„Der Auftragnehmer ist verpflichtet, das Datengeheimnis sowie etwaige berufliche Verschwiegenheitsverpflichtungen zu wahren. Er hat bei der Verarbeitung ausschließlich Beschäftigte einzusetzen, die entsprechend verpflichtet und geschult sind. Er hat insbesondere sicherzustellen, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt werden, die gesetzlichen Datenschutzbestimmungen beachten und die vom Auftraggeber erlangten Informationen nicht unbefugt an Dritte weitergeben oder anderweitig verwerten.

Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für sämtliche vertragsrelevanten Angelegenheiten des Datenschutzes. Der Auftragnehmer hat Frau/Herrn_____ als betrieblichen Datenschutzbeauftragten bestellt.

Der Auftragnehmer ist verpflichtet, ein Verarbeitungsverzeichnis gemäß Art. 30 Abs. 2 DSGVO zu führen. Der Auftragnehmer gewährt dem Landesdatenschutzbeauftragten Zugang zu den Arbeitsräumen und unterwirft sich der Kontrolle nach Maßgabe des Landesdatenschutzgesetzes in seiner jeweiligen Fassung. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontroll- und Ermittlungshandlungen der Aufsichtsbehörde."

6. Unterauftragsverhältnisse

Formulierungsvorschlag:

„Der Auftraggeber genehmigt die gesondert aufgelisteten Unterauftragsverhältnisse, die der Auftragnehmer vor Abschluss dieser Vereinbarung begründet hat. Über Änderungen hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Abschluss neuer Unterauftragsverhältnisse bedarf der vorherigen Zustimmung des Auftraggebers.

Der Auftragnehmer hat dem Unterauftragnehmer dieselben Pflichten aufzuerlegen, die er selbst gegenüber dem Auftraggeber zu erfüllen hat. Der Unterauftragnehmer ist sorgfältig auszuwählen. Der Auftragnehmer haftet gegenüber dem Auftraggeber vollumfänglich für Datenverstöße seiner Unterauftragnehmer."

7. Kontrollrechte des Auftraggebers

Formulierungsvorschlag:

„Der Auftraggeber hat das Recht, vor Beginn und während der Datenverarbeitung die Einhaltung der vom Auftragnehmer sowie von den Unterauftragnehmern getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren oder von zu benennenden Prüfern kontrollieren zu lassen. Das Ergebnis ist zu dokumentieren.

Der Auftragnehmer gewährleistet die Möglichkeit zur Kontrolle. Hierzu weist er dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Der Nachweis kann durch Vorlage aktueller Testats oder durch Berichte unabhängiger Prüfer (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren) erbracht werden.

Haben sich der Auftragnehmer und die von ihm beauftragten Unterauftragnehmer Verhaltensregeln unterworfen oder ein Zertifizierungsverfahren erfolgreich durchlaufen, sind sie verpflichtet, dem Auftraggeber dies nachzuweisen. Zertifikate sind zu aktualisieren.

Der Auftraggeber ist berechtigt, Stichprobenkontrollen durchzuführen. Diese sind anzukündigen. Würde die Ankündigung den Zweck der Prüfung gefährden oder besteht ein dringender Anlass zur Kontrolle, ist eine Ankündigung entbehrlich."

8. Mitteilung bei Verstößen

Formulierungsvorschlag:

„Der Auftragnehmer meldet dem Auftraggeber unverzüglich sämtliche Verstöße gegen Pflichten aus diesem Vertrag. Dies gilt insbesondere bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung bzw. zum Ausschluss möglicher nachteiliger Folgen für die Betroffenen zu ergreifen."

9. Weisungsbefugnis des Auftraggebers

Formulierungsvorschlag:

„Der Auftraggeber ist berechtigt, dem Auftragnehmer jederzeit Weisungen zu erteilen, insbesondere hinsichtlich der Art, des Umfangs und des Zeitpunkts der Verarbeitung von Daten. Die Weisungen des Auftraggebers erfolgen in Textform.

Erachtet der Auftragnehmer eine Weisung des Auftraggebers als rechtswidrig, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Erteilt der Auftraggeber Einzelweisungen bzgl. des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, z.B. Änderungen der technischen und organisatorischen Maßnahmen, werden sie als Antrag auf Leistungsänderung behandelt."

10. Löschung von Daten und Rückgabe von Datenträgern

„Der Auftragnehmer hat dem Auftraggeber sämtliche in seinen Besitz befindlichen personenbezogenen Daten, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, unverzüglich nach Erfüllung des Vertrags oder nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Zusammenarbeit auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ein Zurückbehaltungsrecht ist ausgeschlossen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind vom Auftragnehmer entsprechend der geltenden Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren."

Anlage 9

Muster

Einwilligungserklärung für die Veröffentlichung von Mitarbeiterfotos auf der Betriebswebsite

Für einen persönlicheren und ansprechenderen Internetauftritt möchten wir Ihr Foto im Zusammenhang mit Ihren geschäftlichen Kontaktdaten auf unserer Website www. .de veröffentlichen.

Ich bin damit einverstanden, dass ein Bild, auf dem ich abgelichtet bin, auf o. a. Internetseite veröffentlicht wird.

Mir ist bekannt, dass ich für die Veröffentlichung kein Entgelt erhalte.

Die Zustimmung ist unbefristet erteilt. Sie kann jederzeit widerrufen werden. Der Widerruf ist per E-Mail zu richten an: info@mustermannbetrieb.de oder postalisch an: Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt.

Nach Erhalt des Widerrufs werden wir die betreffenden Daten nicht mehr nutzen und verarbeiten bzw. löschen.

Wir haften nicht dafür, dass Dritte unbefugt den Inhalt der genannten Website für weitere Zwecke nutzen, insbesondere durch Herunterladen und/oder Kopieren von Fotos. Wir versichern, alle zumutbaren Maßnahmen gegen ein solches unerlaubtes Handeln zu unternehmen.

_____

Ort, Datum, Unterschrift

Datenschutzhinweis gemäß Art. 13 DSGVO

Die Veröffentlichung Ihres Fotos beruht auf Ihrer Einwilligung gemäß Artikel 6 Abs. 1 a) DSGVO. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Sie können unseren Datenschutzbeauftragten unter datenschutz@mustermannbetrieb.de oder unter Datenschutzbeauftragter c/o Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, erreichen.

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 10

Muster

Information der Beschäftigten bei Aufnahme der Tätigkeit

Informationen zur Datenverarbeitung gemäß Artikel 13 DSGVO

Die Musterbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, Geschäftsführerin Frau Musterfrau, erhebt Ihre personenbezogenen Daten zum Zweck der Vorbereitung und Durchführung des Beschäftigungsverhältnisses.

Wir erheben von Ihnen zu diesem Zweck folgende personenbezogene Daten:

- Name, Anschrift, Geburtsdatum, Geschlecht, Bankverbindung, Staatsangehörigkeit.

- Angaben zu Ihrer Beschäftigung bei uns sowie zu Ihrer Qualifikation und Ihrem bisherigen Werdegang. Hierzu gehören z.B. Informationen zum höchsten Schulabschluss bzw. zur höchsten Berufsausbildung und Informationen, die Sie uns im Rahmen des Bewerbungsverfahrens überlassen haben.

- Steuer- und sozialversicherungsrechtlich relevante Daten. Dies betrifft u.a. Ihre Steueridentifikationsnummer, Steuerklasse, etwaige Kinderfreibeträge, Familienstand und Angaben zur Konfession (nur sofern steuerrechtlich relevant). Diese und weitere gesetzlich in § 39 e) Einkommenssteuergesetz geregelte Daten erheben wir ggf. auch direkt bei der zuständigen Finanzverwaltung.

- Angaben zu steuerpflichtigen Vorbeschäftigungszeiten im laufenden Kalenderjahr, damit die steuerliche Berechnung entsprechend angepasst werden kann.

- Informationen zu Ihrer Krankenversicherung und ggf. zu weiteren beschäftigungsrelevanten Zusatzversicherungen um etwaigen Zahlungsverpflichtungen und Meldepflichten nachkommen zu können.

- Angaben zu Ihrer Elterneigenschaft. Wir benötigen diese Information, um festzustellen, ob nach § 55 Abs. 3 Sozialgesetzbuch XI ein Beitragszuschlag zur Pflegeversicherung zu entrichten ist.

- Sofern Sie im Zeitpunkt der Einstellung noch nicht volljährig sind, bitten wir Sie ggf. um die Vorlage einer ärztlichen Erstuntersuchungsbescheinigung. Hierzu sind wir nach § 32 Jugendarbeitsschutzgesetz gesetzlich verpflichtet.

- Krankheitszeiten, Abwesenheiten (Urlaub, Sonderurlaub, etc.) oder Arbeitszeiten.

- Angaben über Schwerbehinderungen zwecks Wahrung Ihrer Rechte nach dem Sozialgesetzbuch IX sowie um eine etwaige Ausgleichsabgabe nach § 77 Sozialgesetzbuch IX zu berechnen. Sie müssen diese Angabe erst nach sechs Monaten Beschäftigungszeit beantworten. Vorher ist die Beantwortung freiwillig.

Die Erhebung und Verarbeitung Ihrer personenbezogenen Daten beruht – sofern vorstehend nicht anders angegeben – auf Art. 6 Abs. 1 b) Datenschutz-Grundverordnung (DSGVO) i.V.m. § 26 Bundesdatenschutzgesetz und ist für die Durchführung Ihres Beschäftigungsverhältnisses erforderlich.

Wir übermitteln Daten nur dann an Dritte, sofern dies erforderlich ist und eine Rechtsgrundlage besteht (z.B. an Banken und Steuerberater zur Berechnung und Auszahlung von Lohn und Gehalt, an Sozialversicherungsträger und an Finanzämter zur Erfüllung unserer gesetzlichen Pflichten).

Die von uns über Sie erhobenen Daten werden gelöscht, sobald sie für die Durchführung des Beschäftigungsverhältnisses nicht mehr erforderlich sind oder das Beschäftigungsverhältnis beendet wurde und gesetzliche Aufbewahrungsfristen nicht entgegenstehen.

Wenn Sie in unserem Betrieb als Ausbilder eines Lehrlings eingesetzt werden, werden wir Ihre Daten entsprechend den gesetzlichen Vorgaben an die Handwerkskammer zur Eintragung in die Lehrlingsrolle weiterleiten.

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung der Daten zu fordern.

Sie können unseren Datenschutzbeauftragten unter datenschutz@musterbetrieb.de oder unter Datenschutzbeauftragter c/o Musterbetrieb, Musterstraße 1, 12345 Musterstadt, erreichen. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 11

Muster

Information des Ausbildungsbetriebs an den Auszubildenden bei Abschluss des Lehrvertrags

Informationen zur Datenerhebung gemäß Artikel 13 DSGVO

Die Musterbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, Geschäftsführerin Frau Musterfrau, erhebt Ihre personenbezogenen Daten zum Zweck der Vorbereitung, Abschluss und Durchführung des Lehrvertrags sowie zur Durchführung und Abschluss Ihrer Berufsausbildung.

Wir erheben von Ihnen zu diesem Zweck folgende personenbezogene Daten:

- Name, Anschrift, Geburtsdatum, Geschlecht, Bankverbindung, Staatsangehörigkeit.

- Angaben zu Ihrer Beschäftigung bei uns sowie zu Ihrer Qualifikation und Ihrem bisherigen Werdegang. Hierzu gehören z.B. Informationen zum höchsten Schulabschluss bzw. zur höchsten Berufsausbildung und Informationen, die Sie uns im Rahmen des Bewerbungsverfahrens überlassen haben.

- Steuer- und sozialversicherungsrechtlich relevante Daten. Dies betrifft u.a. Ihre Steueridentifikationsnummer, Steuerklasse, etwaige Kinderfreibeträge, Familienstand und Angaben zur Konfession (nur sofern steuerrechtlich relevant). Diese und weitere gesetzlich in § 39 e) Einkommenssteuergesetz geregelte Daten erheben wir ggf. auch direkt bei der zuständigen Finanzverwaltung.

- Angaben zu steuerpflichtigen Vorbeschäftigungszeiten im laufenden Kalenderjahr, damit die steuerliche Berechnung entsprechend angepasst werden kann.

- Informationen zu Ihrer Krankenversicherung und ggf. zu weiteren beschäftigungsrelevanten Zusatzversicherungen um etwaigen Zahlungsverpflichtungen und Meldepflichten nachkommen zu können.
- Angaben zu Ihrer Elterneigenschaft. Wir benötigen diese Information, um festzustellen, ob nach § 55 Abs. 3 Sozialgesetzbuch XI ein Beitragszuschlag zur Pflegeversicherung zu entrichten ist.

- Sofern Sie im Zeitpunkt der Einstellung noch nicht volljährig sind, bitten wir Sie ggf. um die Vorlage einer ärztlichen Erstuntersuchungsbescheinigung. Hierzu sind wir nach § 32 Jugendarbeitsschutzgesetz gesetzlich verpflichtet.

- Krankheitszeiten, Abwesenheiten (Urlaub, Sonderurlaub, etc.) oder Arbeitszeiten.

- Angaben über Schwerbehinderungen zwecks Wahrung Ihrer Rechte nach dem Sozialgesetzbuch IX sowie um eine etwaige Ausgleichsabgabe nach § 77 Sozialgesetzbuch IX zu berechnen. Sie müssen diese Angabe erst nach sechs Monaten Beschäftigungszeit beantworten. Vorher ist die Beantwortung freiwillig.

Die Erhebung und Verarbeitung Ihrer personenbezogenen Daten beruht – sofern vorstehend nicht anders angegeben – auf Art. 6 Abs. 1 b) Datenschutz-Grundverordnung (DSGVO) i.V.m. § 26 Bundesdatenschutzgesetz und ist für die Durchführung Ihrer Berufsausbildung erforderlich.

Wir übermitteln Daten nur dann an Dritte, sofern dies erforderlich ist und eine Rechtsgrundlage besteht (z.B. an Banken und Steuerberater zur Berechnung und Auszahlung von Lohn und Gehalt, an Sozialversicherungsträger und an Finanzämter zur Erfüllung unserer gesetzlichen Pflichten).

Wir sind zudem gemäß § 30 Handwerksordnung i.V.m. § 36 Abs. 1 Berufsbildungsgesetz verpflichtet, Ihre Daten an die zuständige Handwerkskammer unmittelbar oder über die zuständige Innung an die Handwerkskammer zwecks Eintragung Ihrer Daten in die Lehrlingsrolle zu übertragen.

Die von uns über Sie erhobenen Daten werden gelöscht, sobald sie für die Durchführung des Ausbildungsverhältnisses nicht mehr erforderlich sind oder das Ausbildungsverhältnis beendet wurde und gesetzliche Aufbewahrungsfristen nicht entgegenstehen.

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung der Daten zu fordern.

Sie können unseren Datenschutzbeauftragten unter datenschutz@musterbetrieb.de oder unter Datenschutzbeauftragter c/o Musterbetrieb, Musterstraße 1, 12345 Musterstadt, erreichen. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 12

Muster

Verarbeitungsverzeichnis bezüglich Lohnabrechnung

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis Nr. _____

X Ersterstellung

☐ Änderung eines bestehenden Verzeichnisses

Erstellungsdatum:

Bezeichnung der Verarbeitungstätigkeit: Lohnbuchhaltung

I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO

1. Verantwortlicher Fachbereich/verantwortliche Führungskraft

2. Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter oder des/der weiteren Verantwortlichen

II. Angaben zur Verarbeitungstätigkeit

3. Risikobewertung
Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?

X Nein

☐ Ja

Wenn ja, dann Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Art. 35 DSG-VO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

Lohnbuchhaltung, Gehaltsabrechnung, Archivierung von Lohndaten

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

Art. 6 Abs. 1 Buchst. b) DSGVO (Durchführung des Arbeitsvertrags, Erfüllung vertraglicher Pflichten)

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO

6.1. Betroffene Personengruppen	6.2. Kategorien personenbezogener Daten
- Arbeitnehmer	- Vorname - Name - Anschrift - Kontaktdaten (Telefon, E-Mail etc.) - Arbeitsbeginn - Geburtsdatum - Familienstand - Staatsangehörigkeit - Religionszugehörigkeit - Gehaltssumme

	- sonstige Leistungen

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO	
7.1. Interne Empfänger	_____
7.2. Externe Empfänger	- Finanzbehörden - Sozialversicherungsträger - Steuerberater
7.3. Vertragliche Dienstleister (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen)	_____

8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 e) DSGVO

Übermittlung

X Nein

☐ Ja

Wenn ja, dann: Name des Drittlandes / der internationalen Organisation

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO

Die Daten werden gelöscht, sobald sie zur Erfüllung von Versorgungsansprüchen der jeweiligen Mitarbeiter nicht mehr erforderlich sind.

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

Siehe Datensicherungskonzept.

10.1. Art der eingesetzten Datenverarbeitungsanlagen und Software (optional)
10.2. Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

Anlage 13

Muster

Verarbeitungsverzeichnis bezüglich Personalführung

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis Nr. _____

X Ersterstellung

☐ Änderung eines bestehenden Verzeichnisses

Erstellungsdatum:

Bezeichnung der Verarbeitungstätigkeit: Personalführung

I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO

1. Verantwortlicher Fachbereich/verantwortliche Führungskraft

2. Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter oder des/der weiteren Verantwortlichen

II. Angaben zur Verarbeitungstätigkeit

3. Risikobewertung
Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?

X Nein

☐ Ja

Wenn ja, dann Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Art. 35 DSG-VO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

Sicherstellung ordnungsgemäßer Beschäftigungsverhältnisse sowie ordnungsgemäßer Personalverwaltung/ -Betreuung/ -Führung.

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

Art. 6 Abs. 1 Buchst. b) DSGVO, § 26 Abs. 1 BDSG (Durchführung des Arbeitsvertrags, Erfüllung vertraglicher Pflichten)

§ 26 Abs. 3 BDSG (Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 Abs. 1 DSGVO zum Zweck der Erfüllung gesetzlicher Vorschriften im Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses)

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO	
6.1. Betroffene Personengruppen	**6.2. Kategorien personenbezogener Daten**

- Arbeitnehmer	- Vorname - Name - Postalische Anschrift - Kontaktdaten (Telefon, E-Mail etc.) - Zeugnisse - Lebenslauf - Arbeitsbeginn - Geburtsdatum - Familienstand - Staatsangehörigkeit - Gehaltssumme - sonstige Leistungen **Besonderer Kategorien von Daten gemäß Art. 9 Abs. 1 DSGVO** - Konfession - Krankentage - Gesundheitsbefunde

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO	
7.1. Interne Empfänger	_____
7.2. Externe Empfänger	_____
7.3. Vertragliche Dienstleister (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen)	_____

8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 e) DSGVO

Übermittlung

X Nein

☐ Ja

Wenn ja, dann: Name des Drittlandes / der internationalen Organisation

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO

Nach Ausscheiden des Mitarbeiters werden die Akten vernichtet, soweit die darin vorhandenen Daten nicht für Renten-, Hinterbliebenen oder sonstige Versorgungsansprüche sowie für Nachweispflichten des Bestehens eines Beschäftigungsverhältnisses relevant sind. Sobald keine Versorgungsleistungen mehr zu erbringen sind, werden die Akten restlos vernichtet.

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

Siehe Datensicherungskonzept.

10.1. Art der eingesetzten Datenverarbeitungsanlagen und Software (optional)

10.2. Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

Anlage 14

Muster

Verpflichtung zur Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten

Sehr geehrter Herr/Frau ...,

aufgrund Ihrer Aufgabenstellung sind Sie verpflichtet, die Vertraulichkeit personenbezogener Daten nach Art. 5 Abs. 1 f, Art. 32 Abs. 4 Datenschutz-Grundverordnung (DSGVO), zu denen Sie im Rahmen Ihrer Tätigkeit Zugang erhalten oder über die Sie Kenntnis erlangen, zu wahren. Es ist Ihnen untersagt, unbefugt personenbezogene Daten zu verarbeiten. Diese Verpflichtung besteht nach Beendigung Ihrer Tätigkeit fort.

Verstöße gegen die Vertraulichkeit können nach Art. 83 Abs. 4 DSGVO, §§ 42, 43 Bundesdatenschutzgesetz (BDSG) sowie nach anderen Strafvorschriften (siehe Anlage) mit Freiheits- oder Geldstrafe geahndet werden. Die Verletzung der Vertraulichkeit kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Schweigepflichten begründen.

Eine unterschriebene Zweitschrift dieses Schreibens reichen Sie bitte an die Personalabteilung zurück.

Wir bitten Sie, uns auf der Zweitschrift dieses Schreibens Ihre Verpflichtung zu bestätigen.

Mit freundlichen Grüßen

……

Über die Verpflichtung auf das Datengeheimnis und die sich daraus ergebenen Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung habe ich erhalten.

…… ……..……..

Datum

Rechtliche Grundlagen

Artikel 5 DSGVO

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“); 4.5.2016 L 119/35 Amtsblatt der Europäischen Union DE (1)Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Art. 32 Abs. 4 DSGVO

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Art. 83 Abs. 4 DS-GVO

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

§ 42 BDSG

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder

2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder

2. durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Straf-

verfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43 BDSG

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder

2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeit gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 202d Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.
(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie

2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer

Rechtsanwalts-, Patentanwalts-, Wirtschafts-prüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,

5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist, anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) (weggefallen)

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich ma-

chen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,

2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Anlage 15

Muster

Einwilligungserklärung für den Einsatz von Videokameras in nicht öffentlich zugänglichen Betriebsräumlichkeiten

Um _____ (Bitte die Gründe für die Verwendung von Videokameras einfügen), werden in folgenden Betriebsräumen Videokameras installiert und Videoaufnahmen erstellt. Hierbei ist nicht auszuschließen, dass Sie als Beschäftigte, Beschäftigter gefilmt werden.

Das gefilmte Material wird spätestens 48 Stunden nach Erstellung gelöscht.

Ich bin damit einverstanden, dass ich im Rahmen meiner Tätigkeit gegebenenfalls aber nicht dauerhaft von Videokameras erfasst und gefilmt werde.

Ihre Einwilligung ist unbefristet erteilt. Sie kann jederzeit widerrufen werden. Der Widerruf ist per E-Mail zu richten an: info@mustermannbetrieb.de oder postalisch an: Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt.

_____
Ort, Datum, Unterschrift

Datenschutzhinweis gemäß Art. 13 DSGVO

Die videotechnische Erhebung Ihrer Daten beruht auf Ihrer Einwilligung gemäß Artikel 6 Abs. 1 a) DSGVO. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind, in der Regel jedoch nach 48 Stunden.

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Sie können unseren Datenschutzbeauftragten unter datenschutz@mustermannbetrieb.de oder unter Datenschutzbeauftragter c/o Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, erreichen. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Musterinformation Videoüberwachung

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung[1]

Weitere Informationen erhalten Sie:
- per Aushang (wo genau?)
- an unserer Kundeninformation / Rezeption / Kasse im Erdgeschoss
- (ggf.) zusätzlich im Internet unter …

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:
Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):
Zwecke und Rechtsgrundlage der Datenverarbeitung:
berechtigte Interessen, die verfolgt werden:
Speicherdauer oder Kriterien für die Festlegung der Dauer:

[1] *Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.*

Anlage 17

Aufbewahrungs- und Löschfristen

Die Liste stellt eine Übersicht praxisrelevanter Verfahren dar und erhebt keinen Anspruch auf Vollständigkeit.

Verfahren	**Gesetzliche Aufbewahrungspflicht**	**Gesetzliche Löschfrist**	**Übliche, unverbindliche Löschfrist in der Praxis** (es ist anzunehmen, dass eine längere Datenaufbewahrung i.d.R. nicht erforderlich ist)
Verträge (z.B. Kauf-, Werk-, Leasing- oder Versicherungsvertrag)	6 Jahre (die Frist beginnt nach Beendigung des Vertrags), § 267 HGB, § 147 AO	---	---
steuerrelevante Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanz	10 Jahre, § 147 AO	---	---
Empfangene und versendete Geschäftsbriefe	6 Jahre, § 147 AO	---	---
sonstige steuerrelevante Unterlagen	6 Jahre, § 147 AO	---	---
Mahnvorgänge	6 Jahre § 257 HGB	---	---
Reisekostenabrechnungen	6 Jahre, § 257 HGB	---	---
Bewerbungsunterlagen	---	---	6 Monate, wenn dem Bewerber abgesagt wird.

			3 Jahre nach Beendigung des Arbeitsverhältnisses, wenn der Bewerber den Arbeitsplatz erhält.
Arbeitszeiterfassung (eigene Mitarbeiter sowie Leiharbeitnehmer)	2 Jahre, § 16 Abs. 2 ArbZG	---	3 Jahre nach Beendigung des Arbeitsverhältnisses
Arbeitsverträge	6 Jahre, § 147 AO	---	30 Jahre nach Einstellung (Versorgungsansprüche auch für Hinterbliebene verjähren 30 Jahre nach Entstehung).
Lohn-/Entgeltunterlagen	6 Jahre, § 147 AO	---	---
Unterlagen zu Arbeitsunfällen	5 Jahre, § 24 DGUV Vorschrift 1	---	---
Unterlagen zu Haftungsfällen wegen Sachschäden	---	---	10 Jahre
Unterlagen zu Haftungsfällen wegen Verletzung von Körper oder Gesundheit	---	---	30 Jahre

Anlage 18

Musterformulierung:

Information der Kunden über Weiterleitung der Kundendaten an den Betriebsnachfolger (inhabergeführte Betriebe/Personengesellschaften)

Sehr geehrte(r) Frau/Herr,

als Kunde möchte ich Sie darüber informieren, dass ich den Betrieb zum TT.MM.JJJJ. an Frau/Herrn XY übergeben werde. Ich danke Ihnen für das mir stets entgegengebrachte Vertrauen und freue mich sehr, dass Sie durch Frau/Herr XY auch künftig die gewohnten Leistungen erhalten werden.

Um dies zu ermöglichen, ist es jedoch erforderlich, dass Frau/Herr XY meine über Sie gespeicherten Kundedaten erhält. Sollten Sie dies nicht wünschen, senden Sie mir bitte Ihren Widerspruch postalisch, per Fax oder per E-Mail.

Musterbetrieb, Musterstraße, 12345 Musterstadt

Fax: 123456789

E-Mail: info@musterbetrieb.de

Anderenfalls brauchen Sie nichts zu unternehmen.

Herzlichen Dank für Ihre Unterstützung.

Informationen zur Datenerhebung gemäß Artikel 13 DSGVO

Die Datenübertragung an den Betriebsnachfolger beruht auf Artikel 6 Abs. 1 f) DSGVO. Mit der Datenweitergabe wollen wir Ihnen auch künftig das Leistungsangebot zur Verfügung stellen. Eine Weitergabe der Daten an weitere Dritte findet grundsätzlich nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Datenweiterleitung an den Nachfolgeinhaber jederzeit zu widersprechen. Zudem sind Sie berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 19

Musterformulierung

für Handwerksbetriebe der Gesundheitshandwerke:

Einwilligung zur Übertragung von Kundendaten an den Käufer

Sehr geehrte(r) Frau/Herr,

als Kunde möchte ich Sie darüber informieren, dass ich den Betrieb zum TT.MM.JJJJ. an Frau/Herrn XY übergeben werde. Ich danke Ihnen für das mir stets entgegengebrachte Vertrauen und freue mich sehr, dass Sie durch Frau/Herr XY auch künftig die gewohnten Leistungen erhalten werden.

Um dies zu ermöglichen, ist es jedoch erforderlich, dass Frau/Herr XY meine über Sie gespeicherten Kundendaten erhält. Hierfür benötige und bitte ich Sie um Ihre Zustimmung. Bitte senden Sie die beigefügte Erklärung postalisch, per Fax oder als Scan per E-Mail an mich.

Musterbetrieb, Musterstraße, 12345 Musterstadt

Fax: 123456789

E-Mail: info@musterbetrieb.de

Herzlichen Dank für Ihre Unterstützung.

Einwilligungserklärung

Ja, ich/wir bin/sind damit einverstanden, dass meine/unsere Kundendaten

(Name, Adresse, Faxnummer, E-Mail-Adresse, Vertragshistorie, Bankdaten, Gesundheitsdaten) zum Zweck der Weiterleitung an _____Frau/Herrn XY_____ weitergeleitet und von dieser/diesem zur Fortführung der Kundenbeziehung, insbesondere zur Kontaktaufnahme zwecks Produktwerbung genutzt werden.

Mir/uns ist klar, dass diese Einwilligungen freiwillig und jederzeit widerruflich sind. Der Widerruf ist

per E-Mail zu richten an: info@mustermannbetrieb.de

oder postalisch an: Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt

Nach Erhalt des Widerrufs werden wir die betreffenden Daten nicht mehr nutzen und verarbeiten bzw. löschen.

_____
Ort, Datum, Unterschrift

Die Datenverarbeitung beruht auf Artikel 6 Abs. 1 a) DSGVO. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 20

Musterformulierung:

Einwilligung zur Kontaktaufnahme per E-Mail, Telefon, Fax (Werbung)

Gerne möchten wir, die **Mustermannbetrieb,** Sie telefonisch, per Fax oder E-Mail über Aktionsrabatte, aktuelle Leistungen und Neuigkeiten informieren.

☐ **Ja, ich/wir bin/sind damit einverstanden**, dass meine/unsere Kontaktdaten (Telefonnummer, Faxnummer und E-Mail-Adresse) zum Zweck der Produktwerbung und Informationen zum Leistungsspektrum des Betriebs gespeichert und zur Kontaktaufnahme genutzt werden.

Mir/uns ist dabei klar, dass diese Einwilligungen freiwillig und jederzeit widerruflich sind. Der Widerruf ist

per E-Mail zu richten an: info@mustermannbetrieb.de

oder postalisch an: Mustermannbetrieb, Musterstraße 1, 12345 Musterstadt

Nach Erhalt des Widerrufs werden wir die betreffenden Daten nicht mehr nutzen und verarbeiten bzw. löschen.

_____
Ort, Datum, Unterschrift

Die Datenverarbeitung ist für die Kontaktaufnahme per Telefon, Fax und E-Mail erforderlich und beruht auf Artikel 6 Abs. 1 a) DSGVO. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Sie können unseren Datenschutzbeauftragten unter datenschutz@mustermannbetrieb.de oder unter Datenschutzbeauftragter c/o Mustermannbetrieb, Musterstraße 1, 12345 Musterstadt, erreichen. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.