ZDH
ZENTRALVERBAND DES
DEUTSCHEN HANDWERKS

Leitfaden

Das neue Datenschutzrecht

Was Betriebe künftig zu beachten haben

Gültig ab Mai 2018
Stand November 2017

Abteilung Organisation und Recht

DAS HANDWERK
DIE WIRTSCHAFTSMACHT. VON NEBENAN.

Vorwort

Ab 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 bis zum 25. Mai 2018 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

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“, S. 12.

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“, S. 15).

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 weiter verarbeiten 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“, S. 18.

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 beim Betroffenen direkt erhoben, müssen diesem insbesondere 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“, S. 21.
- **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 Datenverar-

beitung ohne Einwilligung“, S. 4) oder Einwilligung des Betroffenen (siehe hierzu Kapitel 2 „Anforderungen der datenschutzrechtlichen Einwilligung“, S. 6). 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**“**, S. 9).

- 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 (siehe hierzu das beigefügte Muster).

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“, S. 9). 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“, S. 9.

- 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, S. 21).
- **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).

Welcher Handwerksbetrieb muss einen Datenschutzbeauftragten benennen?

Sind im Betrieb mindestens 10 Personen angestellt, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist ein DSB zu benennen. Als automatisierte Verarbeitung gelten z.B.:

- Nutzung digitaler Kundendateien.
- Verwendung von Kundendaten auf einem Tablet-PC oder Smartphone.

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 6. Dokumentationspflichten, S. 18).
- 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 Steuerberater, die für den Betrieb die Steuerklärungen erstellen und dabei z.B. Rechnungen (Adressdaten der Kunden) 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.

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

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 erforderlich und beruht auf Artikel 6 Abs. 1 b) 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 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 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 verwendeten 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 verwendeten 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
☐ 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."