ZENTRALVERBAND
SANITÄR
HEIZUNG KLIMA

LEITFADEN

DATENSCHUTZ IM BETRIEB

Stand: 25.09.2019

Zentralverband Sanitär Heizung Klima
Rathausallee 6, 53757 St. Augustin
Telefon 02241 9299-0
Telefax 02241 21351
info@zvshk.de
www.zvshk.de

Inhalt:

Datenschutz im Betrieb

EINLEITUNG

Ab 25. Mai 2018 gelten in allen Mitgliedstaaten der Europäischen Union neue Datenschutzregeln. Zu diesem Zeitpunkt tritt die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr (EU-Datenschutz-Grundverordnung – DSGVO) vom 27. April 2016 in Kraft. Zeitgleich gelten auch die Änderungen des Bundesdatenschutzgesetz (BDSG).

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 und einigen inhaltlichen 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 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.

In Unternehmen wird man immer wieder mit der sensiblen Frage des Datenschutzes konfrontiert. Datenschutz ist als Grundrecht für Jedermann im Europäischen Recht verankert. Zum Schutz des Einzelnen dürfen personenbezogene Daten danach nur für bestimmte Zwecke und mit Einwilligung des Betroffenen verarbeitet werden oder aufgrund einer gesetzlichen Grundlage. Die Umsetzung dieses Grundrechts erfolgt über die DSGV und das BDSG.

1. GRUNDSÄTZE DES DATENSCHUTZES

1.1 WELCHE DATEN SIND GESCHÜTZT?

1.1.1 Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Insbesondere:

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail Adresse
- Konto-, Kreditkartennummer
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweisnummer, Sozialversicherungsnummer
- Vorstrafen
- genetische Daten und Krankendaten
- Werturteile wie zum Beispiel Zeugnisse
- Eigentumsverhältnisse
- Wohnverhältnisse
- Einkommen.

Hierunter fallen keine Daten über juristische Personen (Unternehmen, Verbände, etc.), es sei denn, diese lassen zwingende Rückschlüsse auf natürliche Personen und deren persönliche Daten zu. Letzteres ist bei Ein-Mann-GmbH und Einzelfirmen regelmäßig der Fall, so dass über diesen Umweg ausnahmsweise auch Unternehmen datenschutzrechtlich Berücksichtigung finden können. Allerdings besteht weitgehend Einigkeit, dass hier ein niedrigeres Schutzniveau anzulegen ist, als bei individuell personenbezogenen Daten.

1.1.2. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

Einige personenbezogene Daten sind besonders schutzwürdig. Dabei handelt es sich um Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten (vgl. Art. 4 Nr. 14, 15 DSGVO), Gesundheitsdaten, Daten zum Sexualleben und Angaben der sexuellen Orientierung. Bezüglich ihrer Verarbeitung bestehen strengere Vorgaben.

1.2. GRUNDSÄTZE BEI DER DATENVERARBEITUNG

Von der DSGVO erfasst wird die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung

personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Ausgenommen sind lediglich Daten für ausschließlich persönliche und familiäre Tätigkeiten.

„Verarbeitung“ meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO). Eine Datennutzung ist nur zulässig, wenn:

- eine gesetzliche Vorschrift sie erlaubt oder
- die betroffene Person in die Nutzung einwilligt.

Soweit der Umgang mit Daten erlaubt ist, gelten folgende Grundsätze:

1.2.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 a) DSGVO)

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

1.2.2. Zweckbindung (Art. 5 Abs. 1 b) DSGVO)

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

1.2.3. Datenminimierung (Art. 5 Abs. 1 c) DSGVO)

Personenbezogene Daten müssen dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

1.2.4 Richtigkeit (Art. 5 Abs. 1 d) DSGVO)

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

1.2.5 Speicherbegrenzung (Art. 5 Abs. 1 e) DSGVO)

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

1.2.6 Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet.

1.2.7. Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.

2. GESETZLICHE ERLAUBNIS

Die Rechtmäßigkeit einer Datenverarbeitung beurteilt sich vor allem nach Artikel 6 DSGVO. Diese Vorschrift wird durch die §§ 22, 24, 26 BDSG ergänzt.

2.1 DATENVERARBEITUNG OHNE EINWILLIGUNG

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 Erfüllung einer **rechtlichen Verpflichtung** (z.B. Abführung von Sozialversicherungsabgaben und Steuern von Mitarbeitern).
- zum **Schutz lebenswichtiger Interessen** der betroffenen Person oder einer anderen natürlichen Person.
- 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).

EXKURS: WERBUNG

Die DSGVO enthält keine spezielle Systematik für die Zulässigkeit von Werbung. Im Grundsatz sind daher die allgemeinen Bestimmungen für die Verarbeitung personenbezogener Daten anzuwenden.
Die Rechtmäßigkeit der Verarbeitung der Daten zu Zwecken der Werbung und des Online Marketings wird somit künftig insbesondere anhand der Vorschrift des Art. 6 Abs. 1 f) DSGVO beurteilt. Danach hat die Verarbeitung „**zur Wahrung der berechtigten Interessen des Verantwortlichen** oder eines

Dritten **erforderlich**“ zu sein, und eine **Interessenabwägung** darf nicht zu dem Ergebnis führen, dass die Verarbeitung unzulässig ist.
Gem. Art. 21 DSGVO kann der Betroffene gegen die Verarbeitung von Daten zu Zwecken der Direktwerbung und gegen das damit verbundene Profiling jederzeit Widerspruch einlegen.
Im Ergebnis ist Werbung daher dann zulässig, wenn die Interessen des Betroffenen gegen eine Werbung nicht überwiegen und er nicht widersprochen hat. Der Werbende muss allerdings nachweisen, dass er eine Interessenabwägung tatsächlich durchgeführt hat und das Ergebnis zu seinen Gunsten ausfällt. Gerade der letzte Punkt dürfte jedoch für die Verantwortlichen nicht unproblematisch sein. In jedem Fall muss die verarbeitende Stelle die in die Abwägung einfließenden Interessen gem. Art. 13 Abs. 1 d) gegenüber dem Betroffenen benennen. Dies kann beispielsweise im Rahmen der Datenschutzerklärung erfolgen.

EXKURS: UNLAUTERE WERBUNG

Die Zulässigkeit der Nutzung von Daten für Werbemaßnahmen ist nicht gleichbedeutend mit der Vereinbarkeit von Werbemaßnahmen mit dem Gesetz gegen unlauteren Wettbewerb (UWG). Zu beachten ist § 7 UWG, der es verbietet, Marktteilnehmer in unzumutbarer Weise zu belästigen. § 7 Abs. 2 stellt dar, welche Werbemaßnahmen stets als unzumutbare Belästigung anzusehen sind.

Hiervon erfasst ist beispielsweise die E-Mail-Werbung ohne vorherige Einwilligung des Adressaten. Wichtige Ausnahmen sind unter § 7 Abs. 3 UWG geregelt. Danach ist die elektronische Werbung dann doch zulässig, wenn

- der Verwender die elektronische Postadresse des Kunden im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden selbst erhalten hat,
- er die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
- der Kunde der Verwendung nicht widersprochen hat und
- der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Grundsätzlich unzulässig ist die Werbung per Telefon, Telefax und SMS, wenn der Adressat als Endverbraucher nicht vorher ausdrücklich eingewilligt hat. Diese Einwilligung muss tatsächlich vorher erfolgen, d. h. die Abfrage der Einwilligung zu Beginn des Telefonats reicht nicht aus. Hier sei darauf hingewiesen, dass die unzulässige Telefonwerbung eine Ordnungswidrigkeit gemäß § 20 UWG darstellen kann.

Gegenüber Unternehmern gilt diese Einschränkung nicht so strikt, so dass lediglich eine mutmaßliche Einwilligung vorliegen muss (§ 7 Abs. 2 Nr. 2 UWG). Beispielsweise bei einer Telefonwerbung im gewerblichen Bereich ist von einer mutmaßlichen Einwilligung auszugehen, wenn die Umstände vor dem Anruf sowie Art und Inhalt der Werbung eine solche nahe legen. Ein ausreichend großes Interesse des Gewerbetreibenden kann schon dann gegeben sein, wenn die Telefonwerbung in einem sachlichen Zusammenhang mit einer bereits bestehenden Geschäftsverbindung steht.

2.2 VERARBEITUNG PERSONENBEZOGENER DATEN VON ARBEITNEHMERN (BESCHÄFTIGTENDATENSCHUTZ)

Die **Verarbeitung personenbezogener Daten von Arbeitnehmern** konkretisiert § 26 BDSG. Im Rahmen des Beschäftigtendatenschutzes reicht es aus, dass die Verarbeitung personenbezogener Daten erfolgt, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen (§ 26 Abs. 7 BDSG), z.B. das handschriftliche Führen von Arbeitszeitguthaben der Mitarbeiter, handschriftliche Geburtstagslisten.

Eine Verarbeitung ist zulässig, wenn es

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

- zur **Ausübung und Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Betriebsvereinbarung ergebenden Rechte und Pflichten der Interessensvertretung** der Beschäftigten erforderlich ist (z.B. Weiterleitung von Arbeitnehmerdaten an den Betriebsrat). Die ausdrückliche Aufnahme der kollektiven Informationsbefugnissen ist neu.

- zur **Aufklärung eines konkreten Straftatverdachts** im Rahmen des Verhältnismäßigkeitsprinzips erforderlich ist (siehe insofern auch unten „Exkurs: Videoüberwachung“).

- bei besonderen Kategorien personenbezogener Daten zur Ausübung von **Rechten oder zur Erfüllung rechtlicher Pflichten** aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes, wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Ein weiterer Rechtfertigungsgrund für die Datenverarbeitung liegt in der **Einwilligung** des Beschäftigten in der Datenverarbeitung (siehe dazu auch unten 3.). Eine Einwilligung kann schriftlich oder elektronisch erfolgen (siehe § 26 BDSG). Dabei ist die grundsätzlich bestehende Abhängigkeit des Beschäftigten vom Arbeitgeber und die Umstände des Einzelfalls zu berücksichtigen. Maßgeblich sind die Arten der verarbeiteten Daten, die Eingriffstiefe, der Zeitpunkt der Einwilligung. Die Einwilligung darf nicht tiefer in die Privatsphäre des Beschäftigten eingreifen, als es der Zweck des Arbeitsvertrages unbedingt erfordert (BAG Urteil vom 11. Mai 1986 – 1 ABP 12784). Dies wird im Zweifel von den Arbeitsgerichten gesondert geprüft.

Hinsichtlich der Mitbestimmungsrechte der Betriebsräte im konkreten Fall sollte die Hilfe der entsprechenden Experten der Handwerksorganisationen hinzugezogen werden.

3. EINWILLIGUNG

Liegt keine gesetzliche Erlaubnis vor, muss der Betroffene in die Verarbeitung seiner Daten eingewilligt haben.

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

3.1 FREIWILLIGKEIT

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.

3.2 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. Im Zweifel trägt die verantwortliche Stelle die Nachweispflicht über die Einwilligung.

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.

3.3 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).
- Die Einwilligung muss sich ausdrücklich auf die Verwertung dieser Daten beziehen.
- 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.

3.4 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.

3.5 AKTIVE ERKLÄRUNG ERFORDERLICH

Die Einwilligung muss aktiv erklärt werden und sollte durch eine eindeutige bestätigende Handlung erfolgen. Dies kann – abgesehen von einer unter-

schriebenen Einwilligung – z.B. durch Anklicken eines Kästchens beim Besuch einer Internetseite geschehen. Stillschweigen, das bloße Hinnehmen bereits angekreuzter 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.

3.6 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.

Weiterführende Unterlagen: Anlage 1: Muster einer Einwilligungserklärung

4. FORMELLE PFLICHTEN VON BETRIEBEN

4.1 ZWECK DER FORMELLEN 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 Datenverarbeitung/-nutzung. 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 DSGVO geregelt. Die Vorschriften werden durch die §§ 32 bis 37 BDSG ergänzt.

4.2 TRANSPARENZGEBOT (ART. 12 DSGVO)

Art. 12 DSGVO 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 prä-

zise, 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.

4.3 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 unten Ziff. 5.

4.4 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 unten Ziff. 6).

4.5 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.

4.6 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.

4.7 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.

4.8 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.

4.9 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 wohl kaum Praxisrelevanz haben.

4.10 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.

4.11 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 unten Ziff. 7.

5. INFORMATIONSPFLICHTEN BEI ERHEBUNG PERSONENBEZOGENER DATEN

5.1 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 DSGVO aufgelistet, die durch §§ 32 und 33 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.

5.2 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 unten Ziff. 8.

- 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 oben Ziff. 2.1) oder Einwilligung des Betroffenen (siehe hierzu oben Ziff. 3). 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 oben Ziff. 4).

- 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.

5.3 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 erhoben (siehe hierzu oben Ziff. 1.1.2)?

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

Exkurs: Internetrecherche über Bewerber

Auch die Internetrecherche über Bewerber stellt eine Datenverarbeitung im Sinne des Datenschutzrechtes dar. Die Suche nach Informationen über Bewerber im world wide web dürfte grds. nach Art. 6 Abs. 1 b) oder f) DSGVO zulässig sein, wenn sie zur Begründung des Beschäftigtenverhältnisses erforderlich ist. Ferner ist davon auszugehen, dass die betroffene Person ihre Daten selbst veröffentlicht haben. Die Datenverarbeitung von selbstveröffentlichen personenbezogenen Daten ist zulässig (Art. 9 Abs. 2 lit. e DSGVO). Das „Googlen" von Bewerberdaten ist damit zulässig.

Etwas anderes gilt, wenn die Daten in einem geschlossen, nicht allgemein zugänglichen Bereich der sozialen Netzwerke (facebook, etc.) erfolgt. Diese Datenerhebung ist unzulässig.

5.4 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).

5.5 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.

5.6 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.

5.7 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.

5.8 DROHEN BEI VERSTÖßEN SANKTIONEN?

Bei Verstößen 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.

6. ERTEILUNG VON AUSKÜNFTEN

6.1 DAS AUSKUNFTSRECHT

Das Datenschutzrecht gewährt Personen, deren Daten verarbeitet werden, umfassende Rechte (siehe hierzu oben Ziff. 4). Eines dieser Rechte ist das Auskunftsrecht. Das Auskunftsrecht ist in Art. 15 DSGVO geregelt und wird durch § 34 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.

6.2 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 wer-den.

6.3 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 oben Ziff. 4).
- Das Bestehen eines Beschwerderechts des Betroffenen bei der Datenschutzaufsichtsbehörde.

6.4 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.

6.5 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.

6.6 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.

6.7 IN WELCHEM ZEITRAHMEN IST DIE AUSKUNFT ZU ERTEILEN?

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

6.8 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.

6.9 MUSTER ZUR AUSKUNFTSERTEILUNG

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

7. DOKUMENTATIONSPFLICHT

7.1 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 Datenschutzgrundverordnung (DSGVO) geregelt.

7.2 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).

EXKURS: VIDEOÜBERWACHUNG

Bei der Zulässigkeit der Videoüberwachung wurde im alten Recht zwischen dem öffentlichen und dem nicht öffentlichen Raum unterschieden. Beim öffentlichen Raum handelt es sich um Bereiche, die ohne Überwindung einer geschlossenen Begrenzung von einem bestimmten Personenkreis betreten werden können und von ihrer Zweckbestimmung her auch dazu bestimmt sind, von der Allgemeinheit betreten zu werden. Dies gilt unabhängig von der Eigentumslage oder der Notwendigkeit einer Anmeldung, Zulassung oder Entrichtung eines Entgelts, Beispiele für öffentliche Räume sind Schalterhallen von Banken, Fußballstadien, Flughäfen, öffentliche Parks, Gärten, Parkplätze, öffentliche Straßen und Wege. Kein öffentlicher Raum sind Werksgelände, Büros oder sonstige Arbeitsräume.

Die offene Videoüberwachung öffentlichen Raumes war für Unternehmen gem. § 6b BDSG (alte Fassung) erlaubt, wenn dies

- zur Wahrnehmung des Hausrechts oder
- zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Es ist davon auszugehen, dass dies im Grundsatz so bleibt und eine Datenerhebung nach Art. 6 Abs. 1 f) DSGVO zulässig bleibt. Es dürfen keine Alternativen zur Videoüberwachung zur Verfügung stehen. In diesen Fällen ist die Videoüberwachung durch geeignete Maßnahmen erkennbar zu machen.

Eine verdeckte Videoüberwachung war nach altem Recht zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist. Auch hier ist von einer Fortgeltung dieser Grundsätze auszugehen.

Im nicht öffentlichen Raum kann eine Videoüberwachung der Beschäftigten daher zulässigerweise nur nach strenger Interessenabwägung erfolgen. Eine heimliche Videoüberwachung kommt überhaupt nur in Frage, wenn

sie das einzige Mittel ist, eine schwere Straftat oder Verfehlung aufzudecken (§ 26 Abs. 1 Satz 2 BDSG). Es muss eine so genannte Notwehrsituation oder notwehrähnliche Lage bestehen.

Aber auch eine offene Videoüberwachung im nicht öffentlichen Raum kommt nur ausnahmsweise in Betracht. Sie ist zulässig, wenn tatsächliche Anhaltspunkte für den Verdacht einer Straftat bestehen und keine milderen Maßnahmen möglich sind. Das Arbeitsverhalten, z. B. die pünktliche Aufnahme der Arbeitstätigkeit, darf dadurch nicht kontrolliert werden. In jedem Einzelfall muss geprüft werden, ob ein berechtigtes Interesse des Arbeitgebers einen so starken Eingriff in das Persönlichkeitsrecht des Beschäftigten erlaubt. Die Aufnahmen von Umkleidekabinen und Toiletten scheiden generell aus.

Soweit die Videoüberwachung zulässig ist, sind die Daten nach Erreichung des Zwecks unverzüglich zu löschen. Werden im öffentlichen Raum Daten einer bestimmten Person zugeordnet, so ist diese über die Überwachung unverzüglich zu benachrichtigen. Bei jeder Betrachtung ist zu beachten, dass die Videoüberwachung in den Schutzbereich des allgemeinen Persönlichkeitsrechtes eingreift.

EXKURS: DATENERHEBUNG ZUR KOORDINIERUNG VON KUNDENDIENSTEINSÄTZEN (ORTUNGSSYSTEME)

Grundsätzlich handelt es sich bei der Ortung eines Arbeitnehmers um die Erhebung und Nutzung von personenbezogenen Daten, so dass die oben dargestellten Anforderungen gelten.

Die Ortung stellt grundsätzlich einen erheblichen Eingriff in das Persönlichkeitsrecht eines Arbeitnehmers dar. Eine gesonderte gesetzliche Regelung gibt es aktuell nicht.

Rechtsgrundlage dürfte nach der gesetzlichen Neuregelung Art. 6 Abs. 1 f) DSGVO. Danach ist die Datenverarbeitung zur erforderlichen Wahrung der berechtigten Interessen des Verantwortlichen (Arbeitgebers) zulässig, wenn nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Bei einer offenen, d.h. dem Arbeitnehmer bekannten GPS-Ortung, muss jedoch ein besonderes Bedürfnis für die Tracking-Maßnahmen vorliegen. Ob das für die Einsatzkoordinierung im normalen Handwerksbetrieb erforderlich ist, muss in jedem Einzelfall geprüft werden.

Bei einer verdeckten GPS-Überwachung ist nach der derzeitigen Rechtsprechung in Anlehnung an die verdeckte Videoüberwachung (siehe oben) eine Notwehrsituation oder eine notwehrähnliche Lage erforderlich. Es dürfen keine milderen Mittel zur Vermeidung zukünftiger Verfehlungen vorliegen.

Alternativ kann der Einsatz der Tracking-Maßnahmen aufgrund einer Einwilligung des Arbeitnehmers zulässig sein (zur Einwilligung s.o. Ziff. 3).

7.3 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 DSGVO zählt die Punkte auf, die in einem Verarbeitungsverzeichnis enthalten sein müssen. Dies sind im Einzelnen:

- Name und die Kontaktdaten der Organisation sowie die Namen ihrer Vertreter (z.B. Präsident, Obermeister, Hauptgeschäftsführer, etc.)

- Name und Kontaktdaten des Datenschutzbeauftragten (DSB).

- Zwecke der Verarbeitung: Z.B. Erfüllung der gesetzlichen Aufgaben unter Angabe des Paragraphen der HwO.

- Beschreibung der Kategorien betroffener Personen: Z.B. Mitglieder, Ansprechpartner aus Verwaltung und Politik, Mitarbeiter, 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 andere öffentliche Stellen).

- 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).

7.4 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Handwerksorganisationen sind verpflichtet, Maßnahmen auf dem Stand der Technik zu ergreifen, um den Risiken zu begegnen, die mit der Datenverarbeitung einhergehen. Diese Pflichten sind vor allem in den Art. 5 Abs. 1 f), 24, 25 und 32 DSGVO geregelt. Darüber hinaus sind ggfs. Vorschriften aus den Landesdatenschutzgesetzen zu berücksichtigen. Es lassen sich thematisch 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).

7.5 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.

8. DER BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE (DSB)

8.1 GESETZLICHE VERPFLICHTUNG

Die Anforderungen an den betrieblichen Datenschutzbeauftragten ergeben sich aus den Artikeln 37 bis 39 DSGVO und § 38 BDSG.

8.2 WELCHER HANDWERKSBETRIEB MUSS EINEN DATENSCHUTZBEAUFTRAGTEN BENENNEN?

Sind im Betrieb mindestens 20 Personen angestellt, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist gem. § 38 Abs. 1 BDSG ein DSB zu benennen. Als automatisierte Verarbeitung gelten z.B.:

- Nutzung digitaler Kundendateien.

- Verwendung von Kundendaten auf einem Tablet-PC oder Smartphone.

- Führen der Mitarbeiterdaten.

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.

8.3 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

- eine 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).

8.4 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 gem. Art. 37 Abs. 7 DSGVO 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.

8.5 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 grundsätzlich wegen der Erfüllung seiner Aufgaben weder abberufen noch benachteiligt werden.

Eine Abberufung kann aber gem. § 6 Abs. 4 i.V.m. § 38 Abs. 2 BDSG aus wichtigem Grund erfolgen. Ein wichtiger Grund können schwerwiegende Verfehlungen in Zusammenhang mit der Funktion als DSB oder eine dauerhafte Arbeitsunfähigkeit sein. Der DSB kann jedoch auch auf Verlangen der Aufsichtsbehörde (§ 40 Abs. 6 BDSG) abberufen werden. Dies kann der Fall sein, wenn der DSB die zur Erfüllung seiner Aufgaben erforderliche Fachkunde nicht besitzt oder ein schwerwiegender Interessenkonflikt vorliegt. Die Abberufung eines internen DSB muss in der Regel unter Abänderung des Arbeitsvertrages erfolgen.

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.

8.6 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 oben Ziff. 7).

- Zusammenarbeit mit der Landesdatenschutzaufsichtsbehörde.

- Ansprechpartner für externe und interne betroffene Personen zu allen Fragen zur Verarbeitung ihrer personenbezogenen Daten.

8.7 WELCHE VERANTWORTUNG TRIFFT EINEN DSB?

Ein DSB ist für die ordnungsgemäße Erfüllung seiner gesetzlichen Aufgaben verantwortlich. Aufgrund der Überwachungsfunktion kann der DSB zivilrechtlich gem. § 280 BGB haften. Für den internen DSB greifen die Grundsätze des innerbetrieblichen Schadensausgleichs.

Ordnungsgelder können nicht gegen einen DSB verhängt werden. Der DSB haftet aufgrund seiner neuen Überwachungsfunktion als Garant gem. § 13 StGB auch strafrechtlich.

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.

8.8 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).

9. DIE VERPFLICHTUNG VON MITARBEITERN AUF DAS DATENGEHEIMNIS

9.1 WARUM SOLLTE VERPFLICHTET WERDEN?

Eine Verpflichtung der Mitarbeiter auf das Datengeheimnis sollte erfolgen, um, den handelnden Personen noch einmal nachdrücklich und sehr deutlich vor Augen zu führen, dass die Verarbeitung personenbezogener Daten streng reglementiert ist. Letztlich dient das Ganze dem Schutz der Betroffenen.

9.2 BESTEHT AUCH NACH DER DSGVO EINE VERPFLICHTUNG?

In der DSGVO findet sich keine explizite Regelung mehr wie noch früher in § 5 BDSG (alte Fassung). Doch das heißt nicht, dass die Verpflichtung auf das Datengeheimnis zukünftig entfallen kann.
Zwar gibt es keinen Artikel, welcher explizit eine Verpflichtung auf das Datengeheimnis vorschreibt oder dieses Datengeheimnis auch nur definiert. Allerdings wird in Art. 32 Abs. 4 DSGVO festgelegt, dass für die Verarbeitung von Daten Verantwortliche und auch Auftragsverarbeiter Schritte unternehmen, „*um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten[…]*„.

Im Grunde ist diese Vorschrift noch strenger als die bisherige, denn der zu verpflichtende Personenkreis wird größer. Bislang waren lediglich Personen zu verpflichten, die „*bei der Datenverarbeitung beschäftigt*“ waren. Letztlich also solche Personen, zu deren Aufgaben es gehört, mit personenbezogenen Daten umzugehen. Zukünftig sind alle die Personen zu verpflichten, „*die Zugang zu personenbezogenen Daten haben*“. Hierzu gehören auch alle die, die beispielsweise Einblick erhalten können.

Allerdings muss konstatiert werden, dass die bisherige konkrete Pflicht zur Verpflichtung auf das Datengeheimnis einer allgemeinen Pflicht „*den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen*„, gewichen ist. Damit wäre beispielsweise auch eine reine Belehrung oder Schulung der Mitarbeiter ausreichend.
Eine schriftliche Verpflichtungserklärung hat aber in jedem Fall den Vorteil, dass der für die Verarbeitung Verantwortliche die unternommenen Schritte nachweisen kann.

Als Vorlage für eine Information der Mitarbeiter kann die Anlage 9 genutzt werden, für eine Verpflichtungserklärung Anlage 10.

10. AUFTRAGSVERARBEITUNG

10.1 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.

10.2 IST DIE AUFTRAGSVERARBEITUNG GESETZLICH GEREGELT?

Die Auftragsverarbeitung ist hauptsächlich in Art. 28 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.

10.3 IST BEI DER AUFTRAGSVERARBEITUNG EINE BESONDERE FORM ZU BEACHTEN?

Art. 28 DSGVO schreibt keine besondere Form vor. Art. 28 DSGVO und § 62 BDSG stellen aber hohe Anforderungen an die Rechtsbeziehung zwischen der Verantwortlichen Stelle und dem Auftragsverarbeiter. Daher sollte schriftlich ein Vertrag abgeschlossen werden, allein wegen der Dokumentation und aus Beweisgründen. Ein Vertrag kann auch in elektronischen Formaten (z.B. PDF) geschlossen werden.

Die verantwortliche Stelle trägt die Auswahlverantwortung, d.h. sie muss sich die Einhaltung des Datenschutzniveaus nachweisen lassen.

10.4 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

10.5 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.

11. SANKTIONEN

11.1 BUßGELD (ART. 83 DSGVO)

Die Missachtung datenschutzrechtlicher Vorschriften kann mit Bußgeldern bis zu 10.000.000 EUR (bei Verstoß gegen einzelne technische und organisatorische Maßnahmen) bzw. bis zu 20.000.000 EUR (bei Verstößen gegen die oben dargestellten Grundsätze der Verarbeitung und gegen die Rechte der betroffenen Personen). Weiterhin können auch strafrechtliche Sanktionen vorgesehen werden.

11.2 HAFTUNG UND RECHT AUF SCHADENSERSATZ (ART. 82 DSGVO)

Entsteht Betroffenen durch einen Verstoß gegen die Vorschriften der DSGVO ein Schaden, kann er diesen von der verantwortlichen Stelle ersetzt verlangen.

Quellenangabe: Das Merkblatt basiert zu großen Teilen auf dem Leitfaden „Das neue Datenschutzrecht“ des ZDH

ANLAGENVERZEICHNIS

Zentralverband Sanitär Heizung Klima
Rathausallee 6, 53757 St. Augustin
Telefon 02241 9299-0
Telefax 02241 21351
info@zvshk.de
www.zvshk.de