ZENTRALVERBAND
SANITÄR
HEIZUNG KLIMA

MERKBLATT

DATENSCHUTZ IM BETRIEB

Stand: 20.11.2013

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

Inhalt:

Datenschutz im Betrieb

EINLEITUNG

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 nationale Umsetzung dieses Grundrechts erfolgt über das Bundesdatenschutzgesetz. In diesem sind einige Pflichten für Unternehmen aufgeführt, die man kennen sollte, um nicht das Risiko eines Bußgeldes einzugehen.

1. GRUNDSÄTZE DES DATENSCHUTZES

1.1 WELCHE DATEN SIND GESCHÜTZT?

1.1.1 Personenbezogene Daten

Personenbezogene Daten sind Daten, die einer bestimmten (natürlichen) Person zugeordnet werden können (§ 3 Abs. 1 BDSG). 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 personenbezogene Daten

Einige personenbezogene Daten sind besonders schutzwürdig. Für diese in § 3 Abs. 8 BDSG aufgeführten Daten (Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) bestehen strengere Vorgaben.

1.1.3 Anonymisierte und pseudonymisierte Daten

Können Daten keiner bestimmten Person zugeordnet werden oder nur mit unverhältnismäßig großem Aufwand, sind sie anonym (§ 3 Abs. 6 BDSG). Soweit jedoch mit bestimmtem Zusatzwissen die Daten doch bestimmten Personen zugeordnet werden können, gelten sie als pseudonymisiert, beispielsweise bei verschlüsselten Daten (§ 3 Abs. 4a BDSG). Anonymisierte und pseudonymisierte Daten unterliegen erleichterten datenschutzrechtlichen Vorgaben.

1.2. GRUNDSÄTZE BEI DER AUTOMATISIERTEN DATENVERARBEITUNG

Die Erhebung, Verarbeitung und Nutzung von Daten (Automatisierte Verarbeitung) ist gem. § 4 BDSG verboten, wenn sie nicht:

- durch Gesetz oder eine andere Rechtsvorschrift, z. B. Betriebsvereinbarung und Tarifvertrag, erlaubt oder angeordnet ist, oder
- der Betroffene seine Einwilligung erklärt hat.

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

1.2.1 Datensparsamkeit (§ 3a BDSG)

Nur das erforderliche Minimum an personenbezogenen Daten darf gesammelt werden. Wenn immer möglich, sollen daher Daten gelöscht oder pseudonymisiert/anonymisiert werden.

1.2.2. Zweckbindung

Daten dürfen nur für den Zweck (bzgl. der Verwendung im nicht öffentlich-rechtlichen Bereich § 28 Abs. 1 Satz 2 BDSG) verwendet werden, für den sie erhoben wurden (dazu unten ausführlich).

1.2.3. Transparenz

Daten dürfen grundsätzlich nur bei dem Betroffenen erhoben werden (§ 4 Abs. 2 Satz 1 BDSG). Durch ergänzende Vorkehrungen muss

sichergestellt sein, dass beim Umgang mit den Daten die Rechte des Einzelnen berücksichtigt werden (beispielsweise Kontroll- und Mitwirkungsrechte).

Da eine strikte Einhaltung der genannten Grundsätze praxisfern wäre und auch nicht immer im Interesse der Betroffenen, gibt es entsprechende Ausnahmen, auf die später im Einzelnen eingegangen wird.

1.3. EINWILLIGUNG

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

Die Einwilligung muss freiwillig und schriftlich erfolgen. Der Betroffene ist auf den Zweck der Datenverarbeitung hinzuweisen und ggf. auf die Folgen der Verweigerung seiner Einwilligung.

Bei der Beurteilung, ob eine Einwilligung freiwillig erfolgt, sind die Gesamtumstände zu beachten.

Die teilweise, insbesondere von Gewerkschaften und den Datenschutzbeauftragten von Bund und Ländern, vertretene Auffassung, wonach im Beschäftigtenverhältnis eine freiwillige Einwilligung per se ausscheide, findet nach Auffassung der Arbeitgeberverbände im Gesetz keine Grundlage. Da der Gesetzgeber bislang bewusst darauf verzichtet habe, eine Sonderreglung für das Arbeitsverhältnis zu schaffen, könne das Argument nicht greifen, wonach im Beschäftigtenverhältnis aufgrund der bestehenden Abhängigkeit immer der Zwang zur Abgabe der Einwilligung bestehe.

1.4. GESETZLICHE ERLAUBNIS

Neben der dargestellten Einwilligung kann automatisierte Datenverarbeitung auch aus anderen Gründen erlaubt sein.

1.4.1. Zweckbindung

Die automatisierte Datenverarbeitung von personenbezogenen Daten für die eigenen Geschäftszwecke ist zulässig, soweit die Zwecke der automatisierten Datenverarbeitung bereits bei der Erhebung festgelegt werden und:

- wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses

mit dem Betroffenen erforderlich ist (zum Beispiel ordnungsgemäße Auftragsbearbeitung, Mängelhaftung, etc.),
- soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (z. B. Rückrufaktionen), oder
- wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Zulässig ist damit insbesondere der Umgang mit Kundendaten, Beschäftigtendaten des eigenen Personals, Daten von Lieferanten und anderen Geschäftspartnern.

1.4.2. Ausnahme von der Zweckbindung

Außerhalb der festgelegten Zwecke ist die automatisierte Datenverarbeitung personenbezogener Daten beispielsweise zulässig zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten oder wenn die Daten allgemein zugänglich sind oder veröffentlicht werden dürften. Dabei muss Interesse an der Zweckänderung das schutzwürdige Interesse des Betroffenen überwiegen. Maßstab ist § 28 Abs. 2 Ziff. 2 BDSG.

1.4.3. Verarbeitung besonderer personenbezogene Daten

Besonders schutzwürdige Daten nach § 3 Abs. 9 BDSG dürfen hingegen nur ganz ausnahmsweise verarbeitet werden, zum Beispiel wenn dies
- zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus psychischen oder rechtlichen Gründen außer Stande ist, seine Einwilligung zu geben (§ 28 Abs. 6 Ziff. 1 BDSG).
- Daten vom Betroffenen offenkundig öffentlich gemacht wurden (§ 28 Abs. 6 Ziff. 2), oder
- zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und das schutzwürdige Interesse des Betroffenen nicht überwiegt (§ 28 Abs. 6 Ziff. 3 BDSG).

Damit ist eine Erhebung und Nutzung dieser Daten in der Regel nur mit Einwilligung des Betroffenen möglich, beispielsweise auch Informationen zu Kunden mit körperlichen Einschränkungen, die für die Beratung im Hinblick auf barrierefreien Umbau für den SHK-Betrieb sinnvoll sein können.

1.4.4. Beschäftigtendaten

Die automatisierte Verarbeitung von Beschäftigtendaten befindet sich seit einigen Jahren in der Diskussion. Trotz verschiedener Anläufe hat der Gesetzgeber die Regelung des § 32 BDSG jedoch noch nicht wie geplant durch ein eigenes Kapitel zum Thema Beschäftigtendatenschutz ersetzt.

Damit gilt zunächst weiterhin, dass Daten eines Beschäftigten nur für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Beschäftigtendaten dürfen nur den Personen der verantwortlichen Stelle zugänglich sein, die diese für ihre Arbeit brauchen.

Die Videoüberwachung von Beschäftigten ist nur unter sehr eingeschränkten Voraussetzungen möglich (s. dort).

Daten, die nicht mehr benötigt werden, sind zu löschen. Dabei sind jedoch die Aufbewahrungsfristen der Abgabenordnung und weiterer Gesetze zu beachten. Eine Veröffentlichung der Daten im Internet oder im Intranet (beispielsweise Geburtstags- oder Telefonlisten) ist nur mit ausdrücklicher Einwilligung des Betroffenen erlaubt oder, wenn dies zur Durchführung des Arbeitsverhältnisses erforderlich ist.

Beschäftigtendaten sind besonders zu sichern und dürfen nicht in einfachen E-Mails übermittelt werden. Ihre Daten sind in Analogie zu den Bestimmungen über die Führung einer Personalakte vor dem Zugriff unberechtigter Dritter zu schützen. Je sensibler die Daten, desto höher das Schutzbedürfnis. So müssen etwa besonders sensible Gesundheitsdaten (z.B. Suchterkrankungen) speziell vor zufälliger Kenntnisnahme Unbefugter gesichert werden. Der Kreis der Zugriffsberechtigten ist in jedem Fall möglichst klein zu halten.

1.5. DATENERHEBUNG

Die Datenerhebung, also das Beschaffen der Daten, hat beim Betroffenen selbst zu erfolgen. Nur ausnahmsweise dürfen Daten auch bei anderen Stellen erhoben werden. Die Ausnahmen sind in § 4 Abs. 2 BDSG geregelt. Am bedeutsamsten dürfte der Fall sein, dass die zu erfüllende Verwaltungsaufgabe ihrer Art nach die Erhebung bei einer anderen Stelle erforderlich macht und daraus aber keine Beeinträchtigung schutzwürdiger Interessen des Betroffenen zu erwarten ist.

Internetrecherche über Bewerber
Auch die Internetrecherche über Bewerber stellt eine Datenverarbeitung im Sinne des Datenschutzrechtes dar und unterliegt den Beschränkungen des BDSG. Die Suche nach Informationen über Bewerber im World Wide Web ist nach § 28 Abs. 1 Nr. 1 BDSG zulässig, wenn sie zur Begründung des Beschäftigtenverhältnisses erforderlich ist. Nicht erforderlich sind private Daten des Bewerbers, so dass ein Zugriff auf die privaten Informationen in sozialen Netzwerken (facebook, Google+, etc.) unzulässig ist. Dies gilt aufgrund des ausdrücklich privaten Charakters dieser Daten (der in der Regel in den Nutzungsbedingungen entsprechender Netzwerke hinterlegt ist). Etwas anderes gilt bei Informationen, die der Betroffene in beruflichen Netzwerken wie Xing oder linkedIn hinterlegt hat.

1.6. DATENÜBERMITTLUNG

Die Übermittlung anonymer oder pseudonymer Daten unterliegt keinen Einschränkungen.

1.7. VIDEOÜBERWACHUNG

Bei der Zulässigkeit der Videoüberwachung ist zwischen dem öffentlichen und dem nicht öffentlichen Raum zu unterscheiden. 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 ist für Unternehmen gem. § 6b BDSG 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 dürfen keine Alternativen zur Videoüberwachung zur Verfügung stehen. In diesen Fällen ist die Videoüberwachung durch geeignete Maßnahmen erkennbar zu machen.

Auch die verdeckte Videoüberwachung ist 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.

Im nicht öffentlichen Raum kann eine Videoüberwachung der Beschäftigten gem. § 32 Abs. 1 Satz 2 BDSG 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. 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.

1.8. 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 unter 1.5. getroffene Beschränkung gilt.

Die Ortung stellt grundsätzlich einen erheblichen Eingriff in das Persönlichkeitsrecht eines Arbeitnehmers dar. Eine gesonderte gesetzliche Regelung gibt es aktuell nicht, auch liegt bislang keine einschlägige Rechtsprechung zur Frage der Zulässigkeit von Ortungsmaßnahmen im Beschäftigtenverhältnis vor.

Rechtsgrundlage entsprechender Tracking-Maßnahmen dürfte § 28 Abs. 1 Nr. 2 bzw. § 32 BDSG sein. Danach ist die Datenerhebung und –nutzung zur erforderlichen Wahrung berechtigter Interessen der verantwortlichen Stelle (Arbeitgeber) zulässig, wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

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 Rettungsdiensten und Feuerwehreinsätzen wird dies derzeit in der Praxis bereits durchgeführt. Hier ist jedoch die besondere Verantwortung und die Gefährdung von Leib und Leben ein Rechtfertigungsgrund.

Bei einer verdeckten GPS-Überwachung ist nach der derzeitigen Rechtsprechung in Anlehnung an die verdeckte Videoüberwachung eine Notwehrsituation oder eine notwehrähnliche Lage erforderlich. Es dürfen keine milderen Mittel zur Vermeidung zukünftiger Verfehlungen vorliegen s. o. 1.7.).

Sonderfall Handyortung: Bei der Ortung muss man zwischen den Verfahren zur Handyortung und den übrigen Ortungsverfahren wie z. B. GPS oder RFID unterscheiden.

Bei der Handyortung muss man unterscheiden, ob das Handy des Arbeitgebers auch zur privaten Nutzung oder nur für den Dienstgebrauch angeboten wird. Für den erstgenannten Fall wird teilweise die Geltung des Fernmeldegeheimnisses angenommen, so dass eine Kontrolle der Daten und der Inhalte, insbesondere der Standorte ohne Einwilligung des Arbeitnehmers in jedem Fall unzulässig wäre (zur Einwilligung s. o. 1.3). Die Verletzung des Fernmeldegeheimnisses würde einen Straftatbestand darstellen. Jedoch haben das Landesarbeitsgericht Berlin-Brandenburg und das Landesarbeitsgericht Niedersachsen in den letzten Jahren entschieden, dass der Arbeitgeber auch mit der Gestattung der privaten Nutzung von Diensthandys kein Dienstanbieter im Sinne des Telekommunikationsgesetzes ist. Mit dieser vorzugswürdigen Ansicht besteht kein Fernmeldegeheimnis und die Kontrolle kann wie bei ausschließlich dienstlicher Gestattung erfolgen.

Alternativ kann der Einsatz der Tracking-Maßnahmen aufgrund einer Einwilligung des Arbeitnehmers zulässig sein (zur Einwilligung s. o. 1.3.).

Dabei muss der Arbeitnehmer vor der Einwilligung auf die damit verbundenen Ziele der Ortung nachweisbar hingewiesen werden.

In jedem Fall sind auch beim Einsatz von Ortungsgeräten die unter 1.2. dargestellten Grundsätze zu beachten, insbesondere Datensparsamkeit und Transparenz.

1.9. DATENNUTZUNG FÜR WERBUNG

Seit dem 01.09.2012 gilt für sämtliche Formen der Werbung gegenüber Verbrauchern der Einwilligungsvorbehalt. D. h., gemäß § 28 Abs. 3 Satz 1 BDSG ist grundsätzlich die Einwilligung des Betroffenen für die Verarbeitung und Nutzung personenbezogener Daten für Werbemaßnahmen erforderlich.

Dies gilt dann nicht, wenn das SHK-Unternehmen für eigene Produkte wirbt (Eigenwerbung). Im Rahmen der Eigenwerbung dürfen folgende personenbezogene Daten auch ohne Einwilligung des Betroffenen genutzt werden (Listendaten):

- Personengruppe
- Beruf
- Name
- Titel
- Akademischer Grad
- Anschrift und
- Geburtsjahr.

Voraussetzung ist allerdings, dass diese Listendaten entweder selbst beim Betroffenen bei Vertragsschluss oder anlässlich eines geschäftlichen Kontaktes erhoben oder allgemein zugänglichen Verzeichnissen entnommen worden sind (§ 28 Abs. 3 Satz 2 Nr. 1 BDSG).

Außerdem darf der Kunde der Nutzung zu Werbezwecken nicht widersprochen haben. Auf dieses Widerspruchsrecht muss der Kunde bereits bei Vertragsschluss hingewiesen werden. Es reicht also nicht, über die Widerspruchsmöglichkeit erst bei der Werbeansprache zu informieren. Daher empfiehlt es sich, einen entsprechenden Hinweis in die Vertrags- bzw. Angebotsunterlagen aufzunehmen, aus denen der Kunde entnehmen kann, dass und wie er der Datennutzung zu Werbezwecken widersprechen kann. Außerdem sollte die Werbung selbst einen solchen Hinweis enthalten. Ein entsprechendes Muster finden Sie als Anlage beigefügt

Ist die Nutzung von Daten für Werbung in der vorgenannten Form zulässig, darf auch so genannte Beipack- oder Empfehlungswerbung durchgeführt werden (§ 28 Abs. 3 Satz 5 BDSG). Flyer von Kooperationspartnern/Herstellern/etc. dürfen zum Beispiel sowohl den eigenen Werbesendungen beigefügt, als auch isoliert versendet werden.

Allerdings muss auch in diesem Fall deutlich hervorgehoben werden, wer Absender dieser Werbung ist, etwa der SHK-Betrieb, der Werbeprospekte eines Herstellers an seine Kunden versendet.

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.

Die Voraussetzungen einer Einwilligung im Sinne des BDSG ergeben sich aus dessen § 4a. Die Beweislast für das Vorliegen der Einwilligung trägt der Werbende.

Die Werbung gegenüber Unternehmen, auch unter Nutzung eines Ansprechpartners, ist hingegen weniger streng reglementiert. Sie ist bereits zulässig, wenn die o. g. Daten unter Nutzung der Geschäftsadresse verwendet werden.

1.10. DATENNUTZUNG IM ADRESSHANDEL

Listendaten dürfen auch an andere Stellen übermittelt werden. Allerdings gelten in solchen Fällen besonders hohe Transparenz-Anforderungen. Die Herkunft der Daten muss für den Betroffenen nachvollziehbar sein. Deswegen ist der Nutzer übermittelter Listendaten verpflichtet, in der Werbung darauf hinzuweisen, woher die übermittelten Daten stammen, dass sie beispielsweise von Adresshändler X erstmals erhoben wurden. Um dies gewährleisten zu können, muss die übermittelnde Stelle die Herkunft der Daten und den Empfänger für mindestens zwei Jahre nach Übermittlung speichern. Sie muss dem Betroffenen diese Informationen auf Nachfrage zur Verfügung stellen. In gleicher Weise muss der Nutzer/Empfänger der Daten speichern, woher die Daten stammen und an wen sie ggf. weitergegeben wurden.

1.11. AUFTRAGSDATENVERARBEITUNG

Von Auftragsdatenverarbeitung spricht man, wenn sich Unternehmen eines Dritten zur Verarbeitung ihrer personenbezogenen Daten bedienen (Outsourcing). Das können insbesondere Werbeagenturen sein, die für das Unternehmen Werbeschreiben an dessen Kunden versenden. In diesen Fällen ist die Übermittlung der zulässig erhobenen Daten uneingeschränkt erlaubt. Auch ist die Lohnabrechnung über ein Steuerbüro im Rahmen der Auftragsdatenverwaltung möglich. In diesen Fällen ist die Übermittlung der zulässig erhobenen Daten uneingeschränkt erlaubt. Allerdings bleibt der Auftraggeber für die Einhaltung der Datenschutzbestimmungen verantwortlich.

Im Rahmen dieser Verantwortung muss der Auftrag schriftlich erteilt werden und einen Mindestkatalog an Angaben enthalten, die in § 11 Abs. 2 BDSG festgehalten sind:

1. der Gegenstand und die Dauer des Auftrages,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrages.

Über die Einhaltung der datenschutzrechtlichen Vorgaben durch den Auftragnehmer hat sich der Auftraggeber regelmäßig zu informieren. Das Ergebnis muss er dokumentieren.

2. RECHTE DER BETROFFENEN

Das Bundesdatenschutzgesetz regelt eine ganze Reihe von Rechten für die Betroffenen.

2.1. AUSKUNFTSRECHT (§ 34 BDSG)

Der Betroffene hat gegenüber der verantwortlichen Stelle ein Auskunftsrecht. Die verantwortliche Stelle hat auf Nachfrage kostenfrei Auskunft zu erteilen über

- die gespeicherten Daten,
- ihre Herkunft,
- an wen die Daten weitergegeben wurden,

- den Zweck der Speicherung.

Hierzu muss sich der Betroffene ausreichend legitimieren können, weshalb eine telefonische Bearbeitung eines solchen Auskunftsbegehrens in der Regel ausscheidet. Denn es muss ausgeschlossen werden können, dass eine nicht autorisierte Person sich auf diesem Wege Zugang zu den Daten verschafft.

Eine Verweigerung der Auskunft kommt nur in ausgesprochenen Ausnahmefällen und nach sorgfältiger Abwägung im Einzelfall in Betracht; für nicht-öffentliche Stellen nur dann, wenn keine Benachrichtigungspflicht (s. § 33 BDSG) besteht.

2.2. BENACHRICHTIGUNG DER BETROFFENEN (§ 33 BDSG)

Werden Daten ohne Kenntnis des Betroffenen erhoben, ist er unverzüglich hierüber zu informieren, wenn nicht eine der in § 33 BDSG aufgeführten Ausnahmen vorliegt.

Bei Beschäftigten- und Kundendaten dürfte in der Regel die Kenntnis des Betroffenen von der Erhebung gegeben sein, so dass auf eine zusätzliche Benachrichtigung verzichtet werden kann.

2.3. BERICHTIGUNG, SPERRUNG ODER LÖSCHUNG (§ 35 BDSG)

Unrichtige Daten sind zu berichtigen. Eine Löschung von Daten kann verlangt werden, wenn die Erhebung unzulässig ist oder die Daten für die Erfüllung des Speicherzwecks nicht mehr erforderlich sind; von nicht-öffentlichen Stellen sind besondere personenbezogene Daten u. a. zu löschen, wenn die verantwortliche Stelle deren Richtigkeit nicht beweisen kann.

Stehen der Löschung ausreichende Gründe entgegen, sind die Daten zu sperren.

2.4. WIDERSPRUCHSRECHT (§ 35 ABS. 5 BDSG)

Betroffene haben das Recht, der automatisierten Verarbeitung ihrer Daten zu widersprechen. Dies gilt auch, wenn die Datenbearbeitung eigentlich zulässig ist. Der Widerspruch ist begründet, wenn das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an der automatisierten Datenverarbeitung überwiegt.

Unabhängig von diesem allgemeinen Widerspruchsrecht gelten für den „Werbewiderspruch“ neben den datenschutzrechtlichen Vorgaben des § 28 BDSG auch die Vorgaben des Gesetzes gegen unlauteren Wettbewerb (s. dazu unter Werbung).

3. PFLICHTEN DER VERANTWORTLICHEN STELLEN

3.1. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (§ 9 BDSG)

Es sind alle technischen und organisatorischen Maßnahmen zu treffen, um den datenschutzrechtlichen Vorgaben nachzukommen. Welche Maßnahmen konkret zu treffen sind, hängt maßgeblich von den Umständen ab, insbesondere der Art der Daten, der Zahl der mit der automatisierten Datenverarbeitung beschäftigten Personen, etc.

Folgende Schutzziele sollen mit den technischen und organisatorischen Maßnahmen erreicht werden (Anlage zu § 9 BDSG):

- Verfügbarkeit und Integrität: Daten aus Verfahren bleiben unversehrt, zurechenbar und vollständig und sind gegen zufällige Zerstörung und Verlust gesichert.
- Vertraulichkeit: Zutritts- und Zugangskontrolle.
- Transparenz und Intervenierbarkeit: Eingabe-, Auftrags- und Weitergabekontrolle und Gewährleistung, dass Betroffene ihre Rechte wirksam ausüben können.
- Unverkettbarkeit: Technisch-organisatorische Gewährleistung der Zweckbindung.

Dabei steigen die Anforderungen an die Maßnahmen mit der Sensibilität der Daten. Als Beispiel sind Beschäftigtendaten zu nennen (s. dort).

3.2. DATENGEHEIMNIS FÜR MITARBEITER (§ 5 BDSG)

Alle mit der automatisierten Datenverarbeitung beschäftigten Mitarbeiter haben sorgsam mit den Daten umzugehen. Ihnen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Hierauf sind die Mitarbeiter bei Aufnahme ihrer Tätigkeit zu verpflichten.

Das Datengeheimnis besteht auch nach Ende der Tätigkeit fort. Mitarbeiter müssen hierüber informiert sein und sollten wissen, dass bei Zuwiderhandeln strafrechtliche Konsequenzen oder Bußgelder drohen können.

Ein Mitarbeiter-Merkblatt zum Datenschutz finden Sie als Anlage.

3.3. MELDEPFLICHT (§ 4D BDSG)

Eine Meldepflicht, wonach die automatisierte Verarbeitung von personenbezogenen Daten durch nicht-öffentliche Stellen dem Landesdatenschutzbeauftragten zu melden ist, dürfte in der Regel für SHK-Betriebe nicht bestehen. Denn Voraussetzung hierfür wäre, dass mehr als neun Personen ständig mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind, und

- kein Datenschutzbeauftragter bestellt ist, oder
- keine Einwilligung des Betroffenen vorliegt, oder
- die Erhebung, Verarbeitung oder Nutzung nicht der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient.

Liegt keine dieser Ausnahmen vor, ist die verantwortliche Stelle meldepflichtig. Das bedeutet, sie muss der zuständigen Aufsichtsbehörde (Landesbeauftragter für Datenschutz) das Verfahren der automatisierten Datenverarbeitung vor Inbetriebnahme melden.

Welche Angaben zu machen sind, ist in § 4e BDSG abschließend aufgeführt:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,

9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

3.4. ÖFFENTLICHES VERFAHRENSVERZEICHNIS (§ 4G BDSG)

Die vorstehend aufgeführten Angaben sind jedermann auf Antrag zugänglich zu machen. Dies gilt für nicht-öffentliche Stellen unabhängig davon, ob eine Meldepflicht besteht. Es bietet sich an, eine entsprechende Information in die Datenschutzhinweise oder das Impressum des eigenen Internetauftrittes einzubinden. Möglich ist aber auch, diese nur auf konkrete Anfrage zugänglich zu machen. Ein entsprechendes Muster finden Sie als Anlage beigefügt.

3.5. PFLICHT ZUR BESTELLUNG EINES DATENSCHUTZBEAUFTRAGTEN (§ 4F BDSG)

In der Regel ist davon auszugehen, dass SHK-Betriebe keinen Datenschutzbeauftragten zu bestellen haben. Denn die Pflicht hierzu besteht nur, wenn in der Regel mehr als neun Personen ständig mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind, und

- keine gesetzliche Verpflichtung vorliegt oder
- eine Einwilligung des Betroffenen vorliegt, oder
- die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertrags- oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient.

3.5.1. Anforderungen an den Datenschutzbeauftragten

Besteht eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, sind die folgenden Punkte zu beachten:

Die Anforderungen an den Datenschutzbeauftragten sind in § 4f Abs. 2 BDSG geregelt.

Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die **zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit** besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden.

Vorhanden sein muss die **Fachkunde, die „erforderlich“ ist**. Dieses Merkmal reduziert die Anforderungen, die effektiv erfüllt sein müssen, oft

erheblich. Erforderlich sind nämlich **nur die Kenntnisse, die in der konkreten Stelle wirklich benötigt werden**.

Fachkunde setzt nicht nur technische, organisatorische und rechtliche Kenntnisse voraus, sondern auch die Kenntnis des Datenflusses und der datenschutzrechtlich relevanten Vorgänge des Unternehmens.

Die obersten Aufsichtsbehörden für den Datenschutz haben dazu folgende Mindestanforderungen definiert[1]:

1. *Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle:*

   - *Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und*

   - *umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,*

   - *Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.*

2. *Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten*

   - *umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,*

   - *Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),*

[1] Beschluss des Düsseldorfer Kreis am 24./25. November 2010

- *betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),*

- *Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle und*

- *Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).*

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse ***bereits zum Zeitpunkt der Bestellung*** *zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.*

Hinweis: Bei den zuständigen Datenschutzaufsichtsbehörden erhalten Sie auf Anfrage Hinweise zu Fachliteratur, Fortbildungseinrichtungen und sonstigen Fortbildungsmöglichkeiten.

Mit **Zuverlässigkeit** ist vor allem die charakterliche Eignung gemeint. Sie wäre etwa ausgeschlossen, wenn der Beauftragte schon datenschutzrelevante Straftaten begangen hat (Schweigepflichtverletzungen usw.).

Ferner spricht die Zuverlässigkeit den Aspekt an, dass keine Interessenkollisionen vorliegen dürfen. Dieses Problem stellt sich dann, wenn der Beauftragte auch noch andere Funktionen ausübt, also nicht hauptamtlich als Beauftragter tätig ist. Beispielsweise ist es nicht zulässig, dass der Leiter der Stelle oder ein Geschäftsführer, ebenso wenig wie der Personal- oder EDV-Chef bestellt werden. Auch enge Verwandte sollten daher nach Möglichkeit nicht bestellt werden.

Dahinter steht jeweils der Gedanke, dass der Beauftragte sonst (jedenfalls zum Teil) Sachverhalte kontrollieren müsste, die er in seiner anderen Funktion geschaffen hat.

Der Datenschutzbeauftragte muss nicht dem Unternehmen angehören. **Auch Externe** können bestellt werden, wenn diese sich den erforderlichen Einblick in das Unternehmen verschaffen können, um ihrer Aufgabe gerecht zu werden.

3.5.2. Unabhängigkeit des Datenschutzbeauftragten - Sonderkündigungsschutz

Im Rahmen seiner Tätigkeit ist der Datenschutzbeauftragte dem Leiter der Stelle direkt unterstellt, was jedoch keinen Einfluss auf die sonstige Hierarchie im Unternehmen hat. In Ausübung seiner Fachkenntnisse ist er völlig weisungsfrei, kann allerdings selbst keine Weisungen erteilen. Dadurch wird der Unternehmensleitung allerdings nicht die Verantwortung für Datenschutzbelange abgenommen. Diese erhält durch den Datenschutzbeauftragten lediglich die erforderliche Unterstützung.

Im Einzelnen haben die obersten Aufsichtsbehörden für den Datenschutz im November 2010 folgende Kriterien im Hinblick auf die Weisungsfreiheit definiert:

Gemäß § 4f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. *DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne Interessenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.*

2. *DSB dürfen wegen der Erfüllung ihrer Aufgaben im Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Abs. 3 Satz 3 ff BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistel-*

lungen und Dokumentationspflichten gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von vier Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von ein bis zwei Jahren empfohlen.

3. *DSB sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit die nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Abs. 4 BDSG).*

Zur zuverlässigen Erfüllung ihrer Aufgaben muss Datenschutzbeauftragten genügend Zeit zur Verfügung stehen. Daher kann es erforderlich sein, dass der Beauftragte von seinen sonstigen Tätigkeiten teilweise entlastet wird.

Hinweis Sonderkündigungsschutz: Die oben dargestellte Ausgestaltung der Kündigungsfristen wurde mittlerweile in § 4f Abs. 3 Satz 5 und 6 gesetzlich konkretisiert: Danach besteht **kein ordentliches Kündigungsrecht** gegenüber dem Datenschutzbeauftragten einer nicht-öffentlichen Stelle bis ein Jahr nach Ende oder Widerruf der Bestellung. Etwas anderes gilt nur, wenn Gründe vorliegen, die eine fristlose Kündigung rechtfertigen.

3.5.3. Art der Bestellung

Die **Bestellung hat grundsätzlich schriftlich durch die Unternehmensleitung zu erfolgen**. Sie kann nur mit Zustimmung des zu Bestellenden erfolgen.

Es besteht keine Pflicht, die Bestellung der Aufsichtsbehörde mitzuteilen. Bei konkreter Anfrage der Behörde besteht jedoch eine Auskunftspflicht.

3.5.4. Widerruf der Bestellung

Bei Vorliegen von Tatsachen, die unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der Interessen beider Vertragsteile eine Fortsetzung der Bestellung unzumutbar machen (beispielsweise weil der Beauftragte die erforderliche Fachkunde nicht besitzt) kann die Bestellung in entsprechender Anwendung des § 626 BGB widerrufen werden.

3.5.5. Aufgaben und Pflichten des Datenschutzbeauftragten

Der Aufgaben- und Pflichtenkreis des Datenschutzbeauftragten wird in § 4g BDSG festgeschrieben.

§ 4g BDSG

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er hat insbesondere:

1. Die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.

2. Die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Im Fall des § 4d Abs. 2 macht der Beauftragte für den Datenschutz die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar. Im Fall des § 4d Abs. 3 gilt Satz 2 entsprechend für die verantwortliche Stelle.

Dabei hängen die jeweiligen Aufgaben stark von der individuellen Betriebsstruktur zusammen.

3.5.6. Aufgaben des Leiters der nicht-öffentlichen Stelle (§ 4g Abs. 2a BDSG)

Besteht aus den oben genannten Gründen in einem Unternehmen oder Verband keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten, fallen dessen Aufgaben in die Zuständigkeit des Unternehmensleiters. Aus diesem Grund müssen auch nicht meldepflichtige Unternehmen bei Einsatz automatisierter Datenverarbeitung immer auf Anfrage ein Verfahrensverzeichnis vorlegen können.

4. RECHTSFOLGEN

4.1. BUßGELD UND STRAFEN

Die Missachtung datenschutzrechtlicher Vorschriften kann mit Bußgeldern bis zu 300.000 Euro geahndet werden. In besonders schweren Fällen kann auch eine strafrechtliche Verfolgung in Frage kommen, die mit einer Strafandrohung bis zu zwei Jahren Freiheitsstrafe bewährt ist.

4.2. SCHADENERSATZANSPRUCH (§§ 7, 8 BDSG)

Entsteht Betroffenen durch schuldhaft unrichtige oder unzulässige automatisierte Datenverarbeitung ein Schaden, kann er diesen von der verantwortlichen Stelle ersetzt verlangen.

Sankt Augustin, 21.11.2013

ANLAGEN

EINWILLIGUNGSERKLÄRUNG DES VERBRAUCHERS FÜR SHK-UNTERNEHMEN (MUSTER)[1]

Der Schutz persönlicher Daten ist für uns sehr wichtig, weshalb wir streng darauf achten, dass unser Umgang mit persönlichen Daten im Einklang mit den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) sowie weiterer Vorschriften des Datenschutzes und des Wettbewerbsrechts steht.

I. Unsere Geschäftsbeziehung berührt in einigen Punkten auch datenschutzrechtliche Aspekte. Insbesondere verarbeiten und nutzen wir die von Ihnen erhobenen Daten wie Name, Anschrift, Telefon, Fax und E-Mail in Verbindung mit den für unser Vertragsverhältnis erheblichen Daten der technischen Gebäudeausrüstung zum Zwecke der Vertragsabwicklung. Außerdem natürlich soweit dies gesetzlich vorgeschrieben ist (beispielsweise Vorhaltefristen gegenüber dem Finanzamt).

   Darüber hinaus verwenden wir Ihre Daten nur, wenn Sie dem nicht widersprechen bzw. ausdrücklich einwilligen.

II. Wir möchten Sie gerne rechtzeitig auf anstehende Termine (beispielsweise Wartungs- und Inspektionstermine) und für Sie interessante neue technologische Entwicklungen aufmerksam machen.

1. Sie sind daher damit einverstanden, dass wir Ihre im Rahmen des bestehenden Auftragsverhältnisses (schriftlich) erhobenen Daten in Verbindung mit den für das Vertragsverhältnis erheblichen Daten der technischen Gebäudeausrüstung zum Zwecke der Werbung (z. B. Übersendung von Kundenmagazinen, Einladung zu Firmenjubiläen, Wartungsintervalle, Abgaswegeüberprüfung und Immissionsschutzmessung, Produktvorstellungen)[2] bis auf Widerruf nutzen. Hierzu können wir Sie auf dem Postwege kontaktieren.

   Sollten Sie damit nicht einverstanden sein, können Sie die vorstehende Klausel bitte ganz oder teilweise streichen.

---

[1] Das Original dieser Einwilligung ist für die Unterlagen des Unternehmens. Dem Kunden sollte eine Kopie ausgehändigt werden.

[2] Die Zweckbestimmung sollte möglichst klar gefasst sein und muss auf den Einzelfall abgestimmt werden.

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

2. Ich bin damit einverstanden, zum unter II.1 aufgeführten Zweck (auch) per

- o E-Mail
- o Telefon
- o Fax
- o SMS (Zutreffendes bitte ankreuzen)

informiert zu werden.

III. Der Datenerhebung und -speicherung kann jederzeit mit Wirkung für die Zukunft widersprochen werden. Sie sind selbstverständlich berechtigt, auf Antrag unentgeltlich Auskunft über die von Ihnen gespeicherten Daten zu erhalten. Hierzu wenden Sie sich bitte an (Kontaktdaten des SHK-Unternehmens/zuständige Person/E-Mail).[3]

Des Weiteren haben Sie das Recht auf Berichtigung, Löschung oder Sperrung unrichtiger Daten. Soweit Daten für abrechnungstechnische und buchhalterische Zwecke genutzt werden, sind sie von einer Kündigung beziehungsweise von einer Löschung nicht berührt.

Ihre Einwilligung können Sie selbstverständlich jederzeit und ohne Begründung ebenfalls mit Wirkung für die Zukunft ändern oder widerrufen.

_____

Ort/Datum/Unterschrift

[3] Bitte bei Bearbeitung entsprechender Anfragen bedenken, dass die Identität der betroffenen Person feststehen muss. Das kann bei telefonischen Anfragen in der Regel nicht ausreichend geprüft und dokumentiert werden. Daher wird teilweise vertreten, dass eine datenschutzrechtlich sichere Bearbeitung von Auskunfts-, Berichtigungs-, Sperr- und Löschungsanträgen nur erfolgen darf, wenn diese handschriftlich unterschrieben sind.

ÖFFENTLICHES VERFAHRENSVERZEICHNIS (MUSTER)

Öffentliches Verfahrensverzeichnis nach § 4 e Bundesdatenschutzgesetz

Name oder Firma der verantwortlichen Stelle:

Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen:

Anschrift der verantwortlichen Stelle:

Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung:

Beispiel für Unternehmen: *Gegenstand des Unternehmens ist die Planung, Errichtung und Instandhaltung von Anlagen der technischen Gebäudeausrüstung. Eine Datenerhebung, -verarbeitung und –nutzung erfolgt zu dem vorstehenden Zweck.*

Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien:

Beispiel für Unternehmen: *Kundendaten, Mitarbeiterdaten sowie Daten von Lieferanten und sonstigen Marktpartnern (Fremdgewerke, Netzbetreiber, Behörden), sofern diese zur Erfüllung des oben genannten Zweckes erforderlich sind.*

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:

Öffentliche Stellen, die Daten aufgrund gesetzlicher Vorschriften erhalten, interne Stellen, die an der Ausführung und Erfüllung der jeweiligen Geschäftsprozesse beteiligt sind, externe Auftragnehmer (Dienstleistungsunternehmen) entsprechend § 11 des Datenschutzgesetzes, externe Stellen, soweit dies zur Erfüllung der oben genannten Zwecke erforderlich ist.

Regelfristen für die Löschung der Daten:

Nach Ablauf der jeweiligen gesetzlichen Aufbewahrungsfristen werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung erforderlich sind. Nicht von gesetzlichen Aufbewahrungspflichten betroffene Daten werden gelöscht, sobald die oben genannten Zwecke weggefallen sind.

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

Geplante Übermittlung in Drittstaaten:

Eine Übermittlung von Daten in Drittstaaten ist nicht geplant.

Allgemeine Beschreibung zur Beurteilung, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind:

Individuelle Angaben der verantwortlichen Stelle. Es reichen kategorisierende Angaben aus, mit denen man sich an der BDSG-Anlage zu § 9 orientieren kann.

Beispiel: *Wir setzen technische Sicherheitsmaßnahmen wie Antivirenprogramme und Firewalls ein. Zudem wird technologisch und organisatorisch gewährleistet, dass nur berechtigte Personen Datenzugriff haben und die Daten vor zufälliger Zerstörung, Manipulation und Verlust geschützt sind. Sowohl die technologischen als auch die organisatorischen Maßnahmen werden ständig geprüft und weiterentwickelt.*

BESTELLUNG ZUM DATENSCHUTZBEAUFTRAGTEN (MUSTER)

Bestellung eines Datenschutzbeauftragten

Sehr geehrte(r) Frau/Herr_____,

hiermit bestellen wir Sie mit sofortiger Wirkung zum Datenschutzbeauftragten gemäß § 4f Bundesdatenschutzgesetz. Sie sind in dieser Funktion der Geschäftsleitung unmittelbar unterstellt und handeln in Anwendung Ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei.

_____ _____

Ort, Datum Unterschrift Geschäftsleitung

Mit der Bestellung bin ich einverstanden

_____

Unterschrift Datenschutzbeauftragte/r

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

DATENSCHUTZ: MITARBEITERINFORMATION UND VERPFLICHTUNGSERKLÄRUNG DATENGEHEIMNIS (MUSTER)[1]

Ihre Tätigkeit in unserem Verband/Unternehmen berührt in einigen Punkten auch datenschutzrechtliche Aspekte. Sie kommen zwangsläufig mit personenbezogenen Daten bzw. sonstigen gesetzlich geschützten Daten in Berührung.

§ 5 des Bundesdatenschutzgesetzes (BDGS) sieht vor, dass der nicht-öffentliche Arbeitgeber Mitarbeiter, die im Betrieb mit der Datenverarbeitung beschäftigt werden, auf das Datengeheimnis zu verpflichten hat.

Hierzu möchten wir Sie zunächst über die wesentlichen Inhalte des Datenschutzes informieren:

Durch Datenschutz soll der einzelne davor geschützt werden, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Das erfordert sorgfältiges und verantwortliches Handeln beim Umgang mit entsprechenden Daten.

Um in unserem Unternehmen die Vorschriften des Datenschutzes und zur Sicherung der Daten sicherzustellen, haben wir entsprechende Maßnahmen getroffen. Hierüber können Sie sich bei Ihrem Vorgesetzten informieren. Außerdem empfehlen wir die Lektüre des umfassenden Merkblattes „Datenschutz“, das wir Ihnen beifügen. Für Ihre persönliche Arbeit bitten wir im Übrigen folgendes zu beachten:

- Halten Sie Ihnen anvertraute Daten unter Verschluss, wenn Sie nicht daran arbeiten. Ihr PC sollte daher bei Ihrer Abwesenheit vom Arbeitsplatz gesperrt sein.

- Bei der Auswahl der Zugangsdaten zu Ihrem PC sollten Sie nur sichere Zugangsdaten wählen. Bitte informieren Sie sich hierzu bei Ihrem Administrator.

- Bitte sehen Sie davon ab, Ihr Passwort in der Nähe des PC zu notieren bzw. aufzubewahren.

[1] Bitte beachten, dass dieses Muster lediglich eine Anregung darstellt, die auf das individuelle Unternehmen und die dortigen Organisationsstrukturen anzupassen ist.

- Datenträger, insbesondere auch Laptops, Smartphones etc. sind auf Reisen besonders zu sichern.

- Bitte versenden Sie keine vertraulichen Informationen per Fax oder ungesicherter E-Mail.

- Die Verwendung von Speichermedien außerhalb des Unternehmensnetzwerkes ist nur nach Rücksprache mit dem Vorgesetzten bzw. soweit vorhanden Datenschutzbeauftragten erlaubt. Dies umfasst auch die Nutzung so genannter Cloud-Lösungen zum Datenaustausch.

Bei Fragen zum Thema Datenschutz bzw. Datensicherung, in Zweifelsfällen und soweit Sie sich als Betroffener in Ihren Datenschutzrechten verletzt sehen, wenden Sie sich bitte an Ihren Vorgesetzten bzw. soweit vorhanden, den Datenschutzbeauftragten.

VERPFLICHTUNG AUF DAS DATENGEHEIMNIS, § 5 BDSG (MUSTER)

Über die einschlägigen Vorschriften des Bundesdatenschutzgesetzes (BDSG) wurde ich in Kenntnis gesetzt. Ich wurde mit den sich daraus ergebenden besonderen Anforderungen an Datensicherheit und Datenschutz bei der Ausübung meiner Tätigkeit vertraut gemacht und auf das Datengeheimnis (§ 5 BDSG) verpflichtet.

Mir ist bewusst, dass es mir untersagt ist, geschützte personenbezogene Daten zu einem anderem als dem zur jeweiligen rechtmäßigen Aufgaben-erfüllung gehörenden Zweck zu verarbeiten und zu nutzen. Diese Pflicht besteht auch nach Beendigung meiner Tätigkeit fort.

Eine Kopie dieser Verpflichtungserklärung und ein Merkblatt zum Datenschutz habe ich erhalten.

_____

Ort, Datum

_____

Unterschrift Arbeitnehmer/in/Auszubildende/r

DATENSCHUTZHINWEIS INTERNET (MUSTER)[2]

Die Durchführung unserer Internet-Aktivitäten berührt in einigen Punkten auch datenschutzrechtliche Aspekte.

Relevante Daten sind im Datenschutz die so genannten persönlichen Daten. Das sind solche Informationen, die man dazu nutzen kann, Ihre Identität zu erfahren. Wichtigste Beispiele sind insbesondere der Name, die Anschrift und die Telefonnummer einer Person.

Insbesondere bei der Vergabe von Zugangsberechtigungen zum internen Bereich und bei Online-Bestellungen werden Daten im Sinne des Datenschutzgesetzes von Ihnen abgefragt und von uns unter Beachtung aller datenschutzrechtlichen Bestimmungen verwertet.[3]

Auf dieser Website werden mit Technologien der (….) Daten zu Marketing- und Optimierungszwecken gesammelt und gespeichert. Aus diesen Daten können unter einem Pseudonym Nutzungsprofile erstellt werden. Hierzu können Cookies eingesetzt werden. Bei Cookies handelt es sich um kleine Textdateien, die lokal im Zwischenspeicher des Internetbrowsers des Seitenbesuchers gespeichert werden. Die Cookies ermöglichen die Wiedererkennung des Internetbrowsers. Die mit den (….)-Technologien erhobenen Daten werden ohne die gesondert erteilte Zustimmung des Betroffenen nicht dazu benutzt, den Besucher dieser Website persönlich zu identifizieren und nicht mit personenbezogenen Daten über den Träger des Pseudonyms zusammengeführt.[4]

Der Datenerhebung und -speicherung kann jederzeit mit Wirkung für die Zukunft widersprochen werden.

Der Schutz persönlicher Daten ist für uns sehr wichtig, weshalb wir streng darauf achten, dass unser Umgang mit persönlichen Daten im Einklang mit den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) sowie weiterer Vorschriften des Datenschutzes im Internet steht.

Sie sind selbstverständlich berechtigt, auf Antrag und unentgeltlich, Auskunft über die von Ihnen gespeicherten Daten zu erhalten. Des Weiteren haben Sie das Recht auf Berichtigung, Löschung oder Sperrung unrichtiger Daten.

---

[2] Die kursiv dargestellten Inhalte sind auf konkrete Sachverhalte gemünzt, während die übrigen Formulierungen allgemeingültig sind.

[3] Alternative für Unternehmen, die Zugangsberechtigungen zu einem internen Bereich (beispielsweise Intranet für Mitarbeiter) oder Online-Shops verwenden.

[4] Soweit automatische Trackingfunktionen eingesetzt werden.

Soweit Daten für abrechnungstechnische und buchhalterische Zwecke genutzt werden, sind sie von einer Kündigung beziehungsweise von einer Löschung nicht berührt.

Links zu Websites anderer Anbieter, die in unserem Angebot enthalten sind, werden von dieser Datenschutzerklärung nicht umfasst. Wir haben keinen Einfluss darauf, dass deren Betreiber die Datenschutzbestimmungen einhalten.