INTERVIEW

Wie der Beipackzettel zum Aspirin

Monika Weitz ist Datenschutzexpertin und berät viele Betriebe zur Umsetzung der Datenschutz-Grundverordnung. Sie kennt die Sorgen der Chefs und erarbeitet mit ihnen praxisnahe Lösungen.

Monika Weitz leitet als Vorstand die Unternehmerfrauen im Handwerk Rhein-Main. Sie ist Kauffrau im Groß- und Außenhandel und Psychologischer Personal Coach. Mit ihrer eigenen Beratungsfirma Unternehmensbaum® berät sie Firmen zu Geschäftsprozessen, Führungsstrukturen und allen Bereichen der kaufmännischen Organisation. Als Dozentin ist sie an verschiedenen Akademien wie ZDH-ZERT, für Unternehmen und Banken tätig. Monika Weitz begleitet in vielen Betrieben die Umsetzung der Datenschutz-Grundverordnung (DSGVO) und ist als Datenschutzbeauftrage gefragt.

Monika Weitz, UFH-Vorstand Rhein-Main, Unternehmensberaterin und Datenschutzbeauftragte

Handwerksblatt: Frau Weitz, seit Mai 2018 gilt die DSGVO, aber viele Unternehmen wissen immer noch nicht, wie sie das Regelwerk in ihrem Betriebsalltag umsetzen sollen. Sie erleben als Datenschutzbeauftragte die konkreten Probleme der Betriebe. Welche Fragen werden Ihnen am häufigsten gestellt?
Weitz: Die erste Frage an mich ist immer: „Brauche ich einen Datenschutzbeauftragten?“ Die DSGVO fordert einen Datenschutzbeauftragten (DSB) ab 250 Mitarbeitern, die Daten verarbeiten. Das Bundesdatenschutzgesetz (BDSG-neu) ist strenger und hat diese Grenze auf zehn Mitarbeiter gesenkt. Oft höre ich von Unternehmen: „Wir sind ja so klein und verarbeiten gar nicht viele Daten, uns betrifft die DSGVO also gar nicht.“ Wenn ich dann nachfrage, stellt sich häufig heraus, dass sehr viele Daten verarbeitet werden. Ob ein DSB gebraucht wird, also mehr als zehn Mitarbeiter Daten verarbeiten, spielt für den durchzuführenden Datenschutz gar keine Rolle.

Handwerksblatt: Der Datenschutz hängt also nicht allein am Datenschutzbeauftragten?
Weitz: So ist es. Viele Unternehmer glauben fälschlicherweise, wenn sie einen DSB haben, ist damit alles erledigt. Das stimmt aber nicht. Der DSB hat nur beratende Funktion. Die Maßnahmen muss der Unternehmer als Verantwortlicher durchführen, er kann sie nicht an den DSB weiterreichen. Das wird oft vergessen. Der Chef ist für alles verantwortlich. Arbeit kann er delegieren, die Haftung aber nicht.
Eine Frage, die mir ebenfalls häufig gestellt wird, ist: Kann die im Betrieb mitarbeitende Unternehmerfrau die Datenschutzbeauftragte sein? Das ist grundsätzlich nur erlaubt, wenn sie nicht in der Geschäftsführung, sondern angestellt arbeitet und weisungsgebunden ist, wie jeder andere Arbeitnehmer. Unter Umständen kann man das nur schwer nachweisen. Dann frage ich immer: Wie ist die Statusprüfung der Rentenversicherung ausgefallen? Hat die DRV eine Bescheinigung ausgestellt, dass die Frau Angestellte ist, kann man sich den Segen des Landesdatenschutzbeauftragten einholen. Als DSB muss sie sich mit IT und der DSGVO auskennen.

Handwerksblatt: Viele denken ja, die DSGVO betreffe nur elektronische Daten.
Weitz: Das ist ein Irrtum! Betroffen sind auch alle Daten auf Papier. Stehen auf einem Auftragszettel zum Beispiel neben dem Namen des Kunden auch Kontaktinformationen zum Ansprechpartner, sind das personenbezogene Daten – und um die geht es. Die DSGVO unterscheidet nicht zwischen unternehmerischen und persönlichen Daten, das sind immer alles personenbezogene Daten.

Handwerksblatt: Offenbar gibt es ja eine Menge Vorgänge, die datenschutzrelevant sind. Wie behalten Unternehmer den Überblick?
Weitz: Wenn ich in einen Betrieb komme, mache ich mit den Verantwortlichen zusammen eine Bestandsaufnahme, wo konkret personenbezogene Daten verarbeitet werden. Und dann erstellen wir einen Maßnahmenplan. Die Anforderungen hängen vom Einzelfall ab. Ein Beispiel aus meiner Praxis: Ein Betrieb nutzt GPS in Firmenautos. Die digitale Überwachung erfolgt anonymisiert mit Wagen-Nummern. Auf den ersten Blick unkritisch. Und dann lagen offen auf dem Tresen im Eingang ein Fahrzeug- und ein Auftragsbuch, in die jede Fahrt mit Namen, Ziel usw. eingetragen werden musste. Das war datenschutzrelevant und ich musste fragen, wie die Bücher gesichert sind und wer sie einsehen kann. Offene Regale sind da schwierig. Oder Videokameras: Neue Hinweis-Schilder sind erforderlich. Werden Menschen gefilmt, braucht man unter Umständen eine Datenschutz-Folgenabschätzung. Wenn ich sehe, dass ein PC nicht mit Passwort geschützt ist oder der Server im Büro frei zugänglich ist, sind dann technische und organisatorische Maßnahmen (TOM) zu ergreifen. Der Datenschutzbeauftragte entscheidet, was konkret passieren muss.

Handwerksblatt: Kann sich der Unternehmer nicht einfach pauschal für alles die Einwilligung des betroffenen Kunden oder Mitarbeiters einholen?
Weitz: Das wäre ganz schlecht! Denn der Einwilligende kann ja auch immer widerrufen. Eine gute Nachricht: Ich brauche gar nicht für alles eine schriftliche Einwilligung! Im ganz normalen Geschäftsverhältnis muss der Kunde nur informiert werden, wie mit seinen Daten umgegangen wird. Das bedeutet, beim ersten Kontakt erhält er einen Hinweis über die Datenverarbeitung und auf die betriebseigene Datenschutz-Information. Die Veröffentlichung erfolgt am besten auf der Website. Es kann in der Fußzeile der E-Mail ein Link gesetzt werden zur Datenschutz-Information und auch auf Angeboten und Rechnungen. Die reine Information in einfacher Sprache genügt hier. Viele haben ja bereits eine Datenschutz-Erklärung auf der Website. Leider werden oftmals Muster verwendet, ohne Prüfung der Inhalte, das ist nicht datenschutzkonform. Auch für die Lohnabrechnung der Mitarbeiter brauche ich keine Einwilligung, denn es betrifft das Beschäftigungsverhältnis. Anders sieht es aus, wenn ich einen Newsletter verschicke oder ein Gewinnspiel machen möchte. Da brauche ich die Einwilligung des Betroffenen schriftlich oder als sogenannte Double-Opt-in-Lösung.

Handwerksblatt: Bei normalem Geschäftskontakt brauche ich also grundsätzlich keine Einwilligung?
Weitz: Genau. Zum Thema Einwilligung gab es zu Beginn der DSGVO ein großes Missverständnis bei manchen Unternehmen. Sie verschickten E-Mails mit dem Inhalt: „Lieber Kunde, wir wollen mit dir in Kontakt bleiben, bitte gib uns dein Okay, dass wir weiter zusammenarbeiten können.“ Von 1.000 Kontakten haben dann nur 200 eine Antwort geschickt. Damit hat sich der Absender selbst ein Bein gestellt, denn die anderen Kunden darf er jetzt nicht mehr kontaktieren. Richtig war die folgende Mail: „Lieber Kunde, wir behandeln deine Daten sorgfältig. Informationen findest du in unserer Datenschutz-Information. Du brauchst gar nichts zu tun. Nur wenn du nicht mehr mit uns arbeiten möchtest, melde dich bitte.“

DAS INTERVIEW FÜHRTE **ANNE KIESERLING**

Es ist wirklich wichtig, dass der Chef die private Nutzung der dienstlichen E-mail-Adresse untersagt.

EIN BESONDERES PROBLEM: E-MAILS UND PRIVATHANDYS

Häufig gibt es Datenschutz-Probleme bei der Nutzung von E-Mails oder privaten Handys der Mitarbeiter. Wer eine E-Mail schreibt, verarbeitet nämlich automatisch Daten. Einen typischen Fall beschreibt Monika Weitz: „Der Chef schickt dem Mitarbeiter eine E-Mail mit dem Namen und der Adresse und Telefonnummer des Kunden auf sein Handy, damit der den Auftrag erledigt. Damit alles korrekt läuft, muss er dafür vorher in einer Smartphone-Nutzungsrichtlinie festlegen, wie mit den Daten umzugehen ist. Diese sollte zum Beispiel beinhalten, dass der Mitarbeiter die Daten auch vertraulich behandelt, dass er sie nicht unaufgefordert weiterleiten darf und wann sie zu löschen sind. Der Mitarbeiter muss informiert und geschult werden und natürlich muss er die Vertraulichkeitserklärung und Nutzungsrichtlinien persönlich unterschreiben. Diese verbleiben dann in der Personalakte.
Bei E-Mails gibt es noch das Problem, dass viele Betriebe E-Mail-Adressen mit den Namen der Mitarbeiter haben. Selbst wenn es sich um Abkürzungen handelt – Anfangsbuchstaben etwa – muss der Chef aus Datenschutzgründen die private E-Mail-Nutzung von Dienstadressen untersagen. Dafür gibt es dann eine Internet-Nutzungsrichtlinie. Wenn ein Mitarbeiter zu Hause arbeitet, ist eine Homeoffice-Nutzungsrichtlinie erforderlich. Der Chef muss die Arbeitnehmer informieren, sensibilisieren und schulen. Auch diese Nutzungsrichtlinien müssen vom Arbeitnehmer unterzeichnet sein und vervollständigen die Personalakte.
Die Einhaltung der Nutzungsrichtlinien muss in Form von regelmäßigen Stichproben überprüft werden. Und dabei geht es nicht nur um die privaten Endgeräte, sondern auch um die geschäftlichen, also etwa Firmenhandys. Die Kontrollen führt der Datenschutzbeauftragte durch. Es ist wirklich wichtig, die privaten E-Mails zu untersagen. Sonst hat der Unternehmer ein Problem mit dem Telekommunikationsgesetz, weil er dann Dienstanbieter ist. Scheidet der Mitarbeiter aus und will, dass seine Daten gelöscht werden, ist die große Frage: Darf er das verlangen oder geht das gegen die geschäftlichen Interessen des Unternehmens? Wenn der Arbeitgeber die Privatnutzung von E-Mails verboten hat, hat er schon mal einen Hebel in der Hand.“

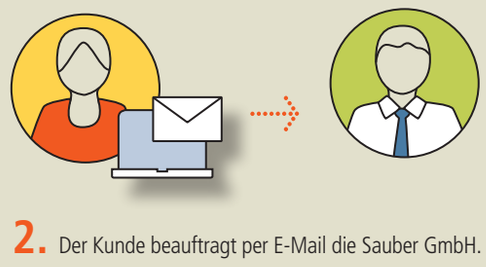
DSGVO soll auf den Prüfstand

Der Bundesdatenschutzbeauftragte Ulrich Kelber will die Kritik an den neuen Datenschutzregeln ernst nehmen. Er kündigte eine Überprüfung an. Denn im kommenden Jahr soll die Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 gilt, evaluiert werden. Bei den deutschen Aufsichtsbehörden sind mittlerweile gut 27.000 Beschwerden eingegangen und es wurden mehr als 12.000 Datenschutzverletzungen gemeldet. Die Risiken umfassender Profile oder von Scorings müssten deutlich stärker in den Fokus gerückt werden, betonte Kelber. „Auf der anderen Seite müssen wir die Kritik an einer wenig zielgerichteten Bürokratisierung ernst nehmen und genau hinschauen, an welchen Stellen die DSGVO entschlackt werden kann, ohne dabei den Datenschutz zu schwächen.“
Unterdessen hat die französische Datenschutzbehörde CNIL gegen den Internetriesen Google wegen Verstößen gegen die DSGVO eine Rekordstrafe von 50 Millionen Euro verhängt.

DSGVO am praktischen Fall – eine Checkliste

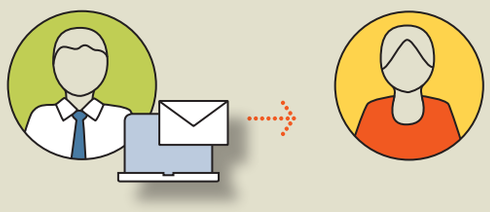
1. Der Kunde hat ein defektes Waschbecken, sucht im Internet einen SHK-Betrieb und findet die Sauber GmbH.

Hat die Website eine korrekte Datenschutzerklärung, ist sie https-verschlüsselt und enthält ein Cookie-Banner?



2. Der Kunde beauftragt per E-Mail die Sauber GmbH.

Die E-Mail ist die Einwilligung zum Mailverkehr.



3. Die Sauber GmbH schreibt eine Auftragsbestätigung per E-Mail an den Kunden.

Hat die E-Mail einen Anhang mit Infos über die Datenschutzerklärung oder verweist sie auf die Website?

4. Der Chef schickt einen Mitarbeiter, um den Auftrag zu erledigen und gibt ihm die Adresse des Kunden auf Zettel oder Handy.

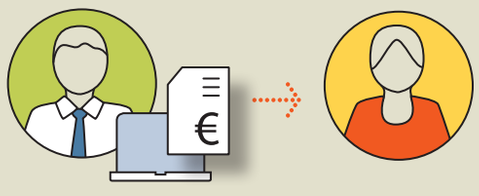
Wurde der Mitarbeiter über die Verwendung der eigenen Daten und der Kundendaten geschult? Hat der Betrieb Nutzungsrichtlinien für Handy, E-Mail, GPS etc.? Hat der Mitarbeiter die Vertraulichkeitserklärung unterzeichnet?

5. Der Hersteller liefert ein neues Waschbecken direkt an den Kunden.

Haben der Hersteller und die Sauber GmbH eine gemeinsame Vereinbarung getroffen, wer die Daten wie verarbeitet? (Info an Kunden darüber ist nicht nötig.)

6. Der Mitarbeiter erledigt den Auftrag. Die Zeiterfassung erfolgt über Stundenzettel oder Stechuhr.

Schickt der Chef die Daten verschlüsselt oder über eine Datenplattform an Steuerberater oder Lohnbüro? Kommt die Abrechnung auch auf gleichem Wege wieder zurück?



7. Der Chef schreibt die Rechnung an der Kunden per E-Mail.

Ist die Information zum digitalen Rechnungesversand erfolgt? Gibt es in der E-Mail einen Fußzeilen-Link zur Datenschutzinformation? Option: Erscheint Hinweis auf Datenschutzinformation auf dem Rechnungsformular?

Grundsätzliches:
Gibt es
- ein Verzeichnis für Verarbeitungstätigkeiten,
- ein Löschkonzept,
- eine Datenschutzfolgenabschätzung
- und einen Auftragsverarbeitungsvertrag?

Grafik: © DHB