handwerk. magazin

www.handwerk-magazin.de

Anleitung:

10 PUNKTE FÜR MEHR SICHERHEIT IN IHREM UNTERNEHMEN

Autoren: Lena Ludwig, PSW GROUP GmbH & Co.KG und Elmar Sommerfeld , LUTOP Datenschutz Akademie GmbH

IMMER AUF DER SICHEREN SEITE

Ausgangslage: Datenschutz und IT-Sicherheit gehen Hand in Hand

Mittlerweile gilt die EU-Datenschutz-Grundverordnung (DSGVO) seit mehreren Jahren. Doch weiterhin lässt die Umsetzung in vielen Unternehmen zu wünschen übrig. Laut Studien durch Wirtschaftsverbände geben im Jahr 2022 immer noch bis zu 60 Prozent der Unternehmer an, dass bei Ihnen der Datenschutz nicht den gesetzlich geforderten Stand wiedergibt. Auch im Bereich Cybersicherheit ist die Bedrohungslage kritisch. Nicht eine Woche vergeht, ohne dass ein weiteres Unternehmen durch einen Hackerangriff betroffen ist. Dabei ist sowohl die Branche als auch die Größe des Opferunternehmens egal, da die Angriffe mittlerweile hochautomatisiert durchgeführt werden.

Gerade in kleinen und mittelständischen Unternehmen wird das Thema Datenschutz und Cybersicherheit oft vernachlässigt – mit gravierenden Folgen für die Unternehmen und Betroffenen. Dabei spielen Bußgelder der Datenschutzaufsichtsbehörden oft eher eine untergeordnete Rolle. Vielmehr wiegt der Reputationsschaden bei Kunden und Partnern schwer und die Wiederherstellungskosten nach einem Datenschutz- oder Cybersicherheitsvorfall sind häufig existenzbedrohend.

Da der Schutz personenbezogener Daten an vielen Stellen eng mit der IT-Sicherheit verbunden ist, sollten Sie als Unternehmer angesichts der aktuell sehr angespannten Cybersicherheitslage beide Themen auf einmal in Angriff nehmen.

Für Handwerksbetriebe ist der Aufwand in Sachen Datenschutz und IT-Sicherheit oft geringer als in vielen anderen Branchen, während die möglichen Schäden ebenso groß sein können. Setzen Sie daher die folgenden zehn Schritte um und sichern Sie sich so einfach gegen die größten Risiken im Bereich Datenschutz und IT-Sicherheit ab.

1. Der Datenschutzbeauftragte (DSB)

Jedes Unternehmen ist – unabhängig von seiner Größe – verpflichtet die Anforderungen an den Datenschutz umzusetzen. Ab 20 Mitarbeitern muss sogar ein eigener Datenschutzbeauftragte (DSB) benannt werden.

Was macht der Datenschutzbeauftragte?
Der DSB berät und informiert die Geschäftsführung und die Mitarbeiter über datenschutzrechtliche Pflichten, gibt Tipps und Hinweise für deren Umsetzung und überwacht die Einhaltung. Daher unterliegt er strengen Verschwiegenheitspflichten. Er übernimmt auch die Kommunikation mit Betroffenen und den Datenschutzaufsichtsbehörden.

Kann jeder Mitarbeiter DSB sein?
Nein. Es darf kein Interessenkonflikt bestehen zwischen den Datenschutzaufgaben und den anderen Aufgaben des Mitarbeiters im Betrieb. Die Inhaber bzw. Gesellschafter, Mitglieder der Geschäftsführung, die Leitung der Marketing-, IT- und Personalabteilung dürfen die Funktion des DSB nicht übernehmen. Dies bedeutet nicht, dass diese Personen sich nicht um die Umsetzung des Datenschutzes kümmern dürfen. Sie dürfen lediglich formal nicht als DSB benannt werden.

Was sind die Konsequenzen bei Nicht-Einhaltung?
Wenn Ihr Unternehmen mehr als 19 Mitarbeiter hat, kann es zu empfindlichen Bußgeldern kommen. Da eine Nicht-Benennung eines Datenschutzbeauftragten als Organisationsverschulden gewertet wird, ist auch eine persönliche Haftung der Geschäftsführung nicht ausgeschlossen.

Experten-Tipp:
Holen Sie sich Expertise ins Haus. Entweder in dem Sie einen Mitarbeiter ausbilden lassen und genügend zeitliche Ressourcen zur fortlaufenden Weiterbildung, Informationsgewinnung und Dokumentation zur Verfügung stellen. Oder indem Sie sich einen externen Experten hinzuziehen, der diese Kenntnisse besitzt und Sie mit Vorlagen und Zuarbeit bei Ihren Pflichten entlastet.

2. Die Webseite

Fast jedes Unternehmen hat mittlerweile seine eigene Website oder einen Online-Auftritt auf Social Media-Plattformen. Da diese Seiten für jedermann zugänglich sind, muss dort besonders Wert auf Datenschutzkonformität gelegt werden. Nicht jeder, der Ihre Webseite besucht, ist Ihnen wohl gesonnen. Auch unzufriedene Kunden, (ehemalige) Mitarbeiter sowie Wettbewerber können hier schnell Angriffspunkte finden. Beispielsweise rollte ab dem Sommer 2022 eine Abmahnwelle durch Deutschland, die alle Websites betraf, die Google Fonts (Schriftarten) dynamisch einsetzten und nicht lokal eingebunden hatten.

Was ist zu tun?
Finden Sie heraus, welche personenbezogenen Daten Ihr Webauftritt verarbeitet. Dabei ist es wichtig, dass Sie sich die folgenden Fragen stellen:

- Haben Sie beispielsweise ein Kontaktformular, einen Online-Shop oder ähnliches?
- Haben Sie einen Newsletter?
- Nutzen Sie Dienste von Dritten – also setzen Sie Dienstleister ein, um Ihre Seite zu betreiben? (Siehe Punkt 4)
- Kommen diese aus dem EU-Ausland? (Siehe Punkt 4)
- Haben Sie Tracking-Technologien im Einsatz – also setzen Sie Cookies ein? (Siehe Punkt 4)
- Verwenden Sie dynamische Karten?
- Oder stellen Sie Videos oder Social Media Content bereit?
- Veröffentlichen Sie Bilder von Ihren Mitarbeitern oder Kunden und Bauprojekte Ihrer Kunden? (Siehe Punkt 8)
- Stellen Sie Bewerbern eine Möglichkeit zur Bewerbung bereit?

Nehmen Sie all diese Informationen in Ihre Datenschutzerklärung auf. Und prüfen Sie vorab, ob die Datenverarbeitungen nach aktuellem Stand rechtmäßig sind. Desweitern müssen Sie prüfen, ob Sie einen Cookie-Banner benötigen.

Sicherheit auf der Website
Sollten Sie auf Ihrer Website die Möglichkeit bereitstellen, Informationen anzugeben (etwa über ein Kontaktformular), benötigen Sie ein Zertifikat zur Verschlüsselung. Ein sogenanntes TLS/SSL-Zertifikat verhindert, dass Daten wie eine Postkarte für jedermann lesbar über das Netz übertragen werden.

Auch sollten Sie immer darauf achten, dass die Seite regelmäßige Sicherheitsupdates erhält, da hier die Wahrscheinlichkeit für die Ausnutzung von Schwachstellen sehr hoch ist.

Pflichtangaben in der Datenschutzerklärung

- Die verantwortliche Stelle – Kontaktinformationen Ihres Unternehmens
- Ansprechpartner für Datenschutz – Kontaktinformationen zu Ihrem Datenschutzbeauftragten oder dem in Ihrem Betrieb Zuständigen für Datenschutzfragen
- Die Zwecke der Verarbeitungen – welche Zwecke werden mit den einzelnen Verarbeitungen verfolgt
- Die Rechtsgrundlagen der Verarbeitungen – auf welcher legalen Grundlage basiert die Verarbeitung auf Ihrer Website
- Gegebenenfalls die Empfänger oder Kategorien von Empfängern – eine Erklärung zu den eingesetzten Dienstleistern
- Gegebenfalls die Übermittlung ins Nicht-EU-Ausland – eine Information zu Empfängern außerhalb des EWR und die eingesetzten rechtlichen Garantien
- Die Speicherdauer oder Kriterien – Welche Speicherdauer Sie bei den Verarbeitungen zu Grunde legen
- Die Betroffenenrechte – eine Information über die Rechte, die Seitenbesuchern aus der DSGVO zustehen
- Das Beschwerderecht – ein Hinweis auf das Recht, sich bei einer Aufsichtsbehörde zu beschweren

Was sind die Konsequenzen bei Nicht-Einhaltung?
Die Konsequenzen können vielfältig sein. Es droht ein Bußgeld durch die Aufsichtsbehörde, die Geschäftsführung hat ein erhöhtes Haftungsrisiko, da geltendes Recht missachtet wurde. Aber auch Abmahnungen etwa durch Wettbewerber sind möglich.

Experten-Tipp
Ihre Website kann jeder sehen, also machen Sie sie sicher. Holen Sie sich Hilfe und befragen Sie Ihren Datenschutzbeauftragten. Auch Ihre Webagentur sollte Ihnen bei der Beantwortung der Fragen weiterhelfen können.

Am einfachsten ist es, wenn Sie eine entsprechende Vorlage für Handwerksbetriebe verwenden, wo die üblichen Verarbeitungen für die Webseite schon dargestellt werden und nur noch angepasst werden müssen. So finden Sie auch leicht heraus, welche Verarbeitungen zulässig sind und welche Sie besser abschalten sollten.

Zusätzlich gibt es eine Vielzahl an Datenschutzerklärungsgeneratoren sowie Anbieter für das Cookie-Management.

Im Übrigen müssen auch für externe Seiten wie z.B. dem Facebook-Auftritt des Unternehmens Datenschutzerklärungen bereitgestellt werden.

3. Datenschutz im Unternehmen

Das A und O für ein sicheres Unternehmen und eine funktionierende Datenschutzorganisation sind Ihre Mitarbeiter. Ihr Unternehmen ist nur so gut geschützt, wie Ihr schwächstes Glied.
Deshalb ist das Wissen über Bedrohungen und eine sichere Datenverarbeitung der wichtigste Punkt, um Ihr Unternehmen zu schützen.

Welche Dokumentation wird benötigt?

Kommunizieren Sie, welchen Stellenwert Datenschutz und Cybersicherheit in Ihrem Unternehmen hat.

- Datenschutzrichtlinie
  Das geht am besten über eine Datenschutzrichtlinie, die für alle Mitarbeiter bindend ist. So erfüllen Sie die Rechenschaftspflichten und geben dem Unternehmen und den Mitarbeiter einen klaren Handlungsrahmen im Datenschutz. So beugen Sie gleichzeitig dem Eindruck vor, dass Ihr Unternehmen den Datenschutz nicht angemessen umsetzt und bieten weniger Angriffspunkte für Beschwerden.

- IT-Sicherheitsrichtlinie
  Erstellen Sie eine Richtlinie und lassen Sie Ihre Mitarbeiter wissen, was Sie mit der vorhandenen IT-Infrastruktur (PCs, Laptops, Tablets, Smartphones, etc.) machen dürfen und was nicht. Definieren Sie, ob private Geräte auch für betriebliche Zwecke genutzt werden dürfen (BYOD – Bring Your Own Device) oder ob Firmengeräte privat genutzt werden dürfen. Legen Sie fest, wo Informationen gespeichert werden und wie der Umgang mit Updates ist. Vor allem, klären Sie über die Gefahren von Phishing-Mails auf, da dies das größte Einfallstor für Verschlüsselungstrojaner oder Datenklau ist.

Wie sensibilisiert man Mitarbeiter?

Alle Mitarbeiter müssen zur Vertraulichkeit verpflichtet werden. Das sollte bereits mit dem Schluss des Arbeitsvertrages erfolgen. Zusätzlich müssen die Mitarbeiter regelmäßig durch entsprechende Schulungen für den Datenschutz und IT-Sicherheit sensibilisiert werden.

Nur so kann sichergestellt werden, dass die Mitarbeiter über die notwendigen Kenntnisse verfügen, um personenbezogene Daten sicher zu verarbeiten und den adäquaten Umgang mit Cybersicherheitsbedrohungen kennen.

Was sind die Konsequenzen bei Nicht-Einhaltung?

Im schlimmsten Fall haben Sie es mit einem Datenschutz- oder Cybersicherheitsvorfall zu tun. Ihre Daten könnten beispielsweise vorab kopiert und danach verschlüsselt worden sein und Hacker fordern Lösegeld für die Entschlüsselung oder drohen mit der

Veröffentlichung. Zu meist werden die Daten auch nach Zahlung des Lösegelds im Darknet veröffentlicht, um durch den Verkauf an Interessierte weiteren Profit zu erwirtschaften.

Aber auch allein schon der Verlust der Arbeitsfähigkeit kann für viele Unternehmen schwierig sein. Sie sind für Ihre Kunden nicht mehr erreichbar, wenn Sie eine digitale Telefonanlage nutzen; wissen nicht, wann Termine vereinbart wurden, wenn Sie einen Online-Kalender zur Terminkoordinierung verwenden; können Produktionsmaschinen nicht mehr bedienen, wenn diese auch über das Internet erreichbar sind und Rechnungen können Sie auch nicht schreiben, weil Sie an Ihre Kundendaten nicht herankommen.

Und sollten Sie trotz besseren Wissens bzw. trotz gesetzlicher Verpflichtung keine Maßnahmen ergriffen haben, greift auch keine Cybersicherheitsversicherung und Sie tragen den Schaden.

Experten-Tipp
Es ist nicht gerade einfach, selbst die gesamte Datenschutzorganisation eines Unternehmens zu entwerfen und niederzuschreiben. Nutzen Sie daher auch hier für Handwerksbetriebe maßgeschneiderte Vorlagen aus der Praxis und passen Sie diese einfach an Ihre Gegebenheiten und Erfordernisse an.

Am einfachsten die Mitarbeiter auf einem aktuellen Stand zu halten, ist es sicherlich durch E-Learnings, da es bei Präsenzterminen immer wieder Mitarbeiter gibt, die urlaubs- oder krankheitsbedingt fehlen und die Schulungen vor Ort deswegen häufig wiederholt oder beim Eintritt eines jeden neuen Mitarbeiters erneut abgehalten werden müssten.

Beim E-Learning für Handwerksbetriebe bekommen die Mitarbeiter einfach einen Link per Email, sehen sich ein Video an, das alles Erforderliche erklärt, sie beantworten kurze Fragen und durch ein Zertifikat kann man die Schulung jederzeit nachweisen. Es reicht nämlich nicht, die Mitarbeiter zu schulen, sondern die Schulung eines jeden Mitarbeiters muss auch nachgewiesen werden können (sogenannte Rechenschaftspflicht). Für die Verpflichtung zur Vertraulichkeit gibt es entsprechende Muster für Handwerksbetriebe.

4. Auftragsverarbeitung

Die meisten Unternehmen heute setzen Dienstleister ein, sei es für den Betrieb der Website, das Buchhaltungsprogramm, das CRM, die Personalverwaltung, den Betrieb der IT oder der Maschinen. Für den Einsatz von Dienstleistern, die mit personenbezogenen Daten in Berührung kommen, sieht die DSGVO verschiedene Anforderungen vor.

Was ist zu tun?
Mit externen Dienstleistern, die mit personenbezogenen Daten in Berührung kommen, sind grundsätzlich sogenannte Auftragsverarbeitungsverträge zu schließen. Die Dienstleister sollten zudem sorgfältig ausgewählt werden, da Probleme mit dem Datenschutz beim Dienstleister auf Ihren Betrieb zurückfallen können.

Warum ist das wichtig?
Der Betrieb, dem die personenbezogenen Daten anvertraut wurden, darf diese nur an externe Dienstleister weitergeben oder ihnen auch nur Einsicht gewähren, wenn ein Auftragsverarbeitungsvertrag vorliegt. Andernfalls liegt ein bußgeldbewährter Datenschutzverstoß vor. Auch dieses Thema kann von den Aufsichtsbehörden geprüft werden.

Was muss in einem Auftragsverarbeitungsvertrag (AVV) geregelt werden?
Die Datenschutz-Grundverordnung sieht spezielle Vorgaben für die Regelungen zwischen Verantwortlichem (Auftraggeber) und Auftragsverarbeiter (Dienstleister) vor:

- Gegenstand der Verarbeitung
- Dauer der Auftragsverarbeitung
- Umfang und Zweck der Datenverarbeitung

- Art der Daten
- Kategorien der betroffenen Personen
- Regelungen zu den Technischen und organisatorischen Maßnahmen (TOM)
- Regelungen zu Berichtigungen, Löschung und Sperrung von Daten
- Pflichten des Auftraggebers
- Pflichten des Auftragnehmers
- Unterauftragsverhältnisse
- Kontrollrechte und Duldungspflichten
- Mitteilungs- und Informationspflichten
- Weisungen
- Rückgabe und Löschung
- Gegebenenfalls Haftung

Der AVV enthält als Anlage zumeist die technischen und organisatorischen Maßnahmen des Auftragnehmers, bzw. die Maßnahmen, auf die sich beide Parteien geeinigt haben.

Was sind die Konsequenzen bei Nicht-Einhaltung?
Sollte kein Auftragsverarbeitungsvertrag geschlossen worden sein, ist ein Bußgeld der Datenschutzaussichtbehörden fällig.

Experten-Tipp
Viele externe Dienstleister bieten schon Auftragsverarbeitungsverträge an, da die Pflicht zum Abschluss der Verträge beide Parteien trifft. Ist dies nicht der Fall, müssen Sie einen solchen Vertrag erstellen. Am besten bedienen Sie sich auch hier wieder entsprechender Vorlagen und Musterverträge. Achten Sie auf die besonderen Bestimmungen für Anbieter aus Drittstaaten (EU-Ausland).

5. Informationspflichten & Betroffenenrechte

Personen, deren Daten verarbeitet werden (Betroffene), müssen bei Erhebung und vor Verarbeitung der Daten transparent darüber informiert werden, was genau mit ihren personenbezogenen Daten passiert. Zu diesen betroffenen Personen zählen im Handwerk hauptsächlich Mitarbeiter, Bewerber, Kunden, Interessenten und Ansprechpartner bei Dienstleistern.

Was ist zu tun?
Wie und worüber die betroffenen Personen zu informieren sind, ist in der DSGVO konkret geregelt. Es muss unter anderem angegeben werden, welche Daten durch wen aufgrund welcher Rechtsgrundlage wie verarbeitet und wie lange gespeichert werden. Zudem ist über die Rechte aufzuklären

- Auskunft
- Berichtigung
- Löschung
- Widerspruch
- Einschränkung
- Datenübertragbarkeit
- Beschwerderecht bei der Datenschutzbehörde

Das heißt, dass Sie diese Informationen an allen Kontaktpunkten zur Verfügung stellen müssen; wie oben in der Checkliste unter Punkt 2 erwähnt in der Datenschutzerklärung auf der Website, bei Vertragsschluss mit Kunden oder Mitarbeitern und beim Erstkontakt mit Bewerbern.

Desweitern sollten Sie sich darauf vorbereiten, dass Mitarbeiter, Kunden oder andere Interessierte bei Ihnen eine Datenschutz-Anfrage stellen – beispielsweise auf Auskunft oder Löschung.

Bereiten Sie eine Musterauskunft vor und gehen Sie Ihre Prozesse durch. Sie haben vier Wochen Zeit, um eine Betroffenenauskunft zu erteilen.

Was sind die Inhalte einer Auskunft?
Die Datenschutz-Grundvorordnung sieht vor, dass über folgende Punkte Auskunft an den Betroffenen gegeben wird:

- die Verarbeitungszwecke
- die Kategorien personenbezogener Daten
- die Empfänger der Daten
- falls möglich die geplante Dauer der Speicherung
- Rechtebelehrung
- Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde
- die Herkunft der Daten
- und gegebenenfalls beim Einsatz von automatisierter Entscheidungsfindung inklusive Profiling, wie dies von statten geht

Was sind die Konsequenzen bei Nicht-Einhaltung?
Der Information der betroffenen Personen wird ein hoher Stellenwert beigemessen, da jeder grundsätzlich selbst darüber entscheiden soll, wer was über ihn weiß. Dies geht nur durch entsprechende Informationen. Daher können auch hier bei fehlenden oder inkorrekten Informationen Bußgelder verhängt werden.
Auch bei der Einhaltung der Betroffenenrechte sind die Aufsichtsbehörden schnell involviert. Allein eine verspätete Auskunft kann zu hohen Bußgeldern und Schadensersatzpflichten gegenüber den Betroffenen führen. Das Auskunftsrecht ist ein einfaches Einfallstor für unzufriedene Kunden, (ehemalige) Mitarbeiter oder Bewerber, wenn kein ausreichender Prozess zum Erteilen der Auskunft besteht.

Experten-Tipp
Auch den Informationspflichten ist relativ einfach nachzukommen, wenn Sie sich Vorlagen und Muster für Handwerksbetriebe besorgen, die bereits die gängigen Datenverarbeitungen im Handwerksbetrieb berücksichtigen und direkt verwendet werden können. Stellen Sie so die erforderlichen Informationen den betroffenen Personen z.B. als Aushang, in Papierform oder elektronisch zur Verfügung. Diese Datenschutzhinweise müssen Sie nur einmal erstellen und können Sie (sofern sich natürlich nichts Entscheidendes ändert) immer wieder verwenden. Alternativ können Sie alles selbst formulieren oder die Arbeit vom externen Datenschutzbeauftragten erledigen lassen. Für die Wahrung der Betroffenenrechte müssen Mitarbeiter so geschult sein, dass sie sicher erkennen, wenn ein Betroffener von einem seiner Rechte Gebrauch macht. Sie müssen zudem wissen, wem sie die Informationen weitergeben müssen. Dies wird auch am einfachsten über die Mitarbeiterschulung (siehe Punkt 3) vermittelt. Wichtig ist darüber hinaus die Einrichtung von erforderlichen Prozessen, um den Betroffenenrechten in der jeweiligen Frist nachzukommen. Für diese Prozesse gibt es entsprechende Merkblätter und Vorlagen, die die Umsetzung erheblich vereinfachen.

6. Das Verzeichnis von Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten soll es sowohl internen als auch externen Personen, die sich mit dem Datenschutz im Unternehmen befassen, erleichtern, einen Überblick über die vorhandenen Datenverarbeitungen und deren Schutzmaßnahmen zu verschaffen. Laut DSGVO müssen Unternehmen erst ab einer Größe von 250 Mitarbeitern ein solches Verzeichnis führen, es sei denn, eine der dort geregelten Ausnahmen trifft zu.

Warum sollten Sie dennoch ein Verzeichnis führen?
Das Verzeichnis von Verarbeitungstätigkeiten muss auf Anfrage den Datenschutzbehörden zur Verfügung gestellt werden. Hier verschafft sich die Behörde bei Beschwerden (häufig durch unzufriedene Kunden und (ehemalige) Mitarbeiter) einen ersten Überblick über den Zustand des Datenschutzes im Betrieb. Auch für das korrekte Beantworten von Betroffenenanfragen ist das Verzeichnis erforderlich (siehe Punkt 5).

Was ist zu tun?
Jedes Unternehmen sollte ein Verzeichnis von Verarbeitungstätigkeiten erstellen und aktuell halten, in dem die Datenverarbeitungen des Betriebes in vorgegebener Form eingetragen sind.

Folgende Inhalte werden in der DSGVO gefordert:

- den Namen und die Kontaktdaten des sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung
- die Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern (auch in Drittländern)
- die geeigneten Garantien bei einem Drittlandtransfer
- Fristen für die Löschung
- technischen und organisatorischen Maßnahmen

Was sind die Konsequenzen bei Nicht-Einhaltung?
Nur wer weiß, welche personenbezogenen Daten im Unternehmen verarbeitet werden, kann diese auch angemessen schützen. Das Führen eines Verzeichnisses der Verarbeitungstätigkeiten spricht immer für eine vernünftige Datenschutzorganisation – auch wenn Sie gesetzlich nicht dazu verpflichtet sein sollten.

Experten-Tipp
Bei der Erstellung und Führung eines Verzeichnisses gibt es Mindestangaben, die gemacht werden müssen. Auch hier gibt es vorausgefüllte Vorlagen und Muster für die typischerweise im Handwerksbetrieb vorkommenden Verarbeitungen.

7. Technische und organisatorische Maßnahmen (TOM)

Um Ihre Daten zu Kunden, Interessenten, Mitarbeitern, Bewerbern und Dienstleistern zu schützen, müssen technische und organisatorische Maßnahmen getroffen werden, die dem Risiko entsprechend angemessen sind. Hierzu zählen auch Maßnahmen der IT-Sicherheit nach aktuellem Stand der Technik. Zudem sind diese Maßnahmen zu dokumentieren.

Was ist zu tun?
Sollten Sie ein Verzeichnis der Verarbeitungstätigkeiten erstellt haben, gehen Sie nun einfach Schritt für Schritt Ihre Verarbeitungen durch und dokumentieren Sie, welche Sicherheitsmaßnahmen Sie für den Schutz der personenbezogenen Daten getroffen haben. Das können sowohl technische Maßnahmen sein, wie Firewall, starke Passwörter etwa mit Zwei-Faktor-Authentisierung, Verschlüsselung oder Backups. Oder organisatorische Maßnahmen wie themenspezifische Richtlinien, Mitarbeiterschulung und Verpflichtung auf Vertraulichkeit.

Was sind die Konsequenzen bei Nicht-Einhaltung?
Diese Dokumentation muss auf Verlagen der Aufsichtsbehörde vorgelegt werden und es können bei unzureichenden Maßnahmen Bußgelder verhängt werden, vor allem, wenn diese zu Risiken für die personenbezogenen Daten geführt haben. Das Treffen der Maßnahmen schützt auch den Betrieb besser vor Hackerattacken oder minimiert mögliche Schäden, zum Beispiel wenn durch einen Cyberangriff alle Daten des Unternehmens verschlüsselt sind und die Angreifer ein „Lösegeld" für die Entschlüsselung verlangen. Haben Sie hier zuvor einen funktionierenden Datensicherungs- und Wiederherstellungsprozess (Backup) implementiert, werden Sie sehr erleichtert sein.

Experten-Tipp
Fast alle Handwerksbetriebe haben ähnlichen Risiken vorzubeugen, so dass sich Muster und Vorlagen empfehlen. Vergleichen Sie, welche Maßnahmen in Ihrem Unternehmen existieren und an welchen Stellen Sie noch nachbessern müssen. Es gibt einige Maßnahmen, die mit geringem Aufwand das Schutzniveau maßgeblich steigern können. Sie müssen nicht alles gleichzeitig umsetzen, sondern können nach Risiko priorisieren und schrittweise vorgehen.

8. Bildrechte

Gerade Handwerksbetriebe stellen auf ihrer Website gern das Team vor oder es gibt eine Galerie zu erfolgreichen Referenzprojekten. Damit Sie das auch zukünftig ohne Bedenken tun können, müssen Sie sich an die Vorgaben aus der DSGVO halten.

Was ist zu tun?
Werden Bild-, Ton- oder Videoaufnahmen von Personen (vor allem Mitarbeiter, Kunden, Interessenten) angefertigt, ist in allen Fällen eine Einwilligung oder ein Vertrag erforderlich. Aber auch beim Veröffentlichen von Bildern von Immobilien muss der Betroffene vorab gefragt werden.

Holen Sie sich daher vor der Verwendung von Bild-, Ton- oder Videoaufnahmen von den betreffenden Personen schriftliche Einwilligungen ein. Damit erklärt sich die betroffene Person mit der Verwendung der Bild-, Ton- und Videoaufnahmen für den vereinbarten Zweck einverstanden.

Wie bereits erwähnt kann in manchen Fällen auch ein Vertrag sinnvoll sein.

Was sind die Konsequenzen bei Nicht-Einhaltung?
Gerade unzufriedene (ehemalige) Mitarbeiter, Kunden oder Dienstleister nutzen den Datenschutz oft als Druckmittel gegen das Unternehmen. Oft geht es dann auch um Bild-, Ton- oder Videoaufnahmen, die ohne (nachweisbare) Einwilligung verwendet wurden. Können Sie keine Einwilligung nachweisen, liegt ein Datenschutzverstoß vor und Bußgeld und Schadensersatzforderungen können erhoben werden.

Experten-Tipp
Setzen Sie immer auf eine dokumentierte Einwilligung oder einen schriftlichen Vertrag. Auch wenn sich zum Zeitpunkt der Aufnahmen alle Beteiligten mündlich einverstanden erklärt haben, müssen Sie als Unternehmen im Streitfall den Nachweis erbringen. Am besten verwenden Sie auch hier Muster für die Einwilligungen oder den Vertrag, die bereits für die Zwecke der Verwendung von Bild-, Ton- oder Videoaufnahmen von Personen im Handwerksbetrieb angepasst sind.

9. Videoüberwachung

Viele Handwerksbetriebe überwachen das Betriebsgelände mit Videoanlagen, um sich vor Diebstahl und Vandalismus zu schützen. Oft werden die Aufnahmen auch zur Aufklärung von Rangierschäden oder Arbeitsunfällen verwendet.

Was ist zu tun?
Videoüberwachung ist mit entsprechenden Hinweisschildern zu kennzeichnen und auf Zulässigkeit zu überprüfen. Hier gibt es nur enge Grenzen, in denen die Videoüberwachung erlaubt ist. Es sind klare Regeln für die Speicherdauer der Aufnahmen (in der Regel sind bis zu 72 Stunden zulässig) und die Zugriffsrechte zu treffen.

Auch muss eine Datenschutzfolgenabschätzung durchgeführt werden. Diese ist immer notwendig, wenn eine Datenverarbeitung eine schwerwiegende Einschränkung der Rechte und Freiheiten der Betroffenen nach sich ziehen kann. Die Datenschutzfolgenabschätzung ist eine Risikoanalyse in Bezug auf die Gefahren für Betroffene, die durch eine Videoüberwachung entstehen können.

Was sind die Konsequenzen bei Nicht-Einhaltung?
Aufsichtsbehörden achten verstärkt auf das Thema der Videoüberwachung, da es immer mehr Videokameras gibt und man als Unternehmen wirklich gute Gründe haben muss, eine Videoüberwachung rechtskonform einsetzen zu dürfen. Auch beim Thema Videoüberwachung werden oft Bußgelder verhängt, sogar im Privatbereich.

Experten-Tipp
Bei dem Thema Videoüberwachung sind mehrere Punkte zu beachten, die sich in der Praxis am besten anhand einer Checkliste zur Videoüberwachung für Betriebe im Handwerk abhaken lassen. Dabei geht es um Zulässigkeit der Videoüberwachung, Interessensabwägung, Informationspflichten, Speicherdauer, Zugriffsrechte sowie die entsprechende Dokumentation.

10. Datenschutz- und Cybersicherheitsvorfälle

Je früher ein Datenschutz- oder Cybersicherheitsvorfall erkannt wird, umso größer ist die Chance, den Schaden für die betroffenen Personen und den Betrieb gering zu halten. Ein Grund mehr, warum Ihre Mitarbeiter gut informiert sein müssen.

Was ist zu tun?
Definieren Sie Meldewege für Ihre Mitarbeiter. So können Sie sicherstellen, dass Sie rechtzeitig von einem Vorfall erfahren. Nur dann können Sie die Situation bewerten und falls erforderlich Gegenmaßnahmen ergreifen.

Was sind die Konsequenzen bei Nicht-Einhaltung?
Der Versuch, eine Datenschutzverletzung zu vertuschen, führt zu Bußgeldern, so dass das Melden des Vorfalls immer die bessere Alternative ist.

Experten-Tipp
Zuerst ist wichtig, dass die Mitarbeiter wissen, was überhaupt eine Datenpanne bzw. ein Datenschutzverstoß ist, damit dieser erkannt und an die Geschäftsführung oder den Datenschutzbeauftragten gemeldet werden kann. Dieses Wissen kann am besten in der Mitarbeiterschulung (siehe Punkt 3) vermittelt werden. Die Geschäftsführung und der Datenschutzbeauftragte prüfen und entscheiden dann, ob es sich um einen Verstoß handelt, der meldepflichtig ist. Ist dies der Fall, muss innerhalb von 72 Stunden eine Meldung an die Aufsichtsbehörde erfolgen. Diese entscheidet dann, ob die Betroffenen ebenfalls über den Vorfall informiert werden müssen.

Hier sollten Unternehmer Prozesse implementieren, um einen rechtskonformen Umgang mit und Datenschutzverstößen sicherzustellen. Der Meldeprozess muss im Unternehmen definiert und bekannt sein. Verfügbare Checklisten und Dokumente, die diesen Prozess abbilden, helfen auch hier den Betrieben im Handwerk mit diesen Herausforderungen umzugehen.

Fazit
Wie Sie sehen, können Sie die meisten der zehn Punkte mit einfachen Vorlagen und Mustern für Datenschutz und IT-Sicherheit in Handwerksbetrieben umsetzen und so die größten Schwachstellen und Risiken beseitigen.
Entsprechende Hilfen und Dokumente speziell für Datenschutz und IT-Sicherheit für Handwerksbetriebe finden Sie über die Suchmaschine Ihres Vertrauens.

Die Autoren:

- **Lena Ludwig – Leiterin PSW Consulting bei der PSW GROUP GmbH & Co.KG**
  Als Datenschutzexpertin und externe Datenschutzbeauftragte steht Lena Ludwig für einen pragmatischen Ansatz bei der Umsetzung der Datenschutzanforderungen. Sie unterstützt Unternehmen dabei, den für sie passenden Weg zu finden. Die PSW GROUP besteht aus verschiedenen Teilen, die wichtige Aspekte in der IT-Sicherheit abdecken: Auf www.psw-consulting.de erfahren Sie alles zu Datenschutz, Informationssicherheit und TISAX®. Auf www.psw-group.de erfahren Sie mehr zu SSL- und Internet Security-Produkte und auf www.psw-training.de sehen Sie Möglichkeiten der Qualifizierung Ihrer Mitarbeiter.

- **Elmar Sommerfeld – Rechtsanwalt und Geschäftsführer der LUTOP Datenschutz Akademie GmbH**
  Seit über zehn Jahren hilft er Unternehmen, ihren Datenschutz kostengünstig, intern mit eigenen Mitarbeitern zu organisieren und Datenschutzbeauftragte auszubilden. Die LUTOP Datenschutz Akademie hat sich auf Ausbildungen, Kurse und Arbeitshilfen wie Vorlagen und Software im Bereich Datenschutz und IT-Sicherheit spezialisiert und hilft Unternehmen, ihren Datenschutz kostengünstig zu organisieren. Einen Überblick über die Lösungen finden Sie unter www.datenschutzbeauftragter-ausbildung.com.