



# Datenschutz für Handwerksbetriebe

In 10 Schritten durch das neue Datenschutzrecht

Referent: Peter Masluk  
FV SHK Bayern



# Schritt 1 :Kundeninformation

- Nach Art 13 DSGVO müssen gegenüber Kunden Informationspflichten erfüllt werden
- Diese sind exemplarisch:
- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- Zweck der Datenverarbeitung
- Rechtsgrundlage der Datenverarbeitung
- Widerspruchsrecht, Lösungsrecht, Auskunftsrecht des Kunden



## Schritt 2: Mitarbeiterinfo- Datenverarbeitung

- Bei Abwesenheit PC am Arbeitsplatz sperren
- Verwenden von sicheren Zugangsdaten
- Passwort geheim halten und nicht am Arbeitsplatz notiert aufbewahren
- Datenträger, Laptops, Smartphones sind unterwegs besonders zu sichern
- Vertrauliche Informationen nicht per Fax oder ungesicherter E-Mail
- Verwendung von Speichermedien oder Cloud nur nach Rücksprache mit DSB



## Schritt 3: Mitarbeiterverpflichtung auf das Datengeheimnis

- Nachweis, dass der Mitarbeiter über die datenschutzrechtlichen Belange informiert worden ist ( vgl Datenschutzinformation Mitarbeiter)
- Hinweis, dass personenbezogene Daten nur zweckgebunden verarbeitet und benutzt werden dürfen



## Schritt 4: Datenschutzerklärung auf der Webseite

- Hinweis, dass und welche personenbezogene Daten ( Name, Adresse, Telefonnummer, IP Nummer) gespeichert werden
- Hinweis, dass der Einsatz von Cookies stattfindet und welche Art der Cookies
- Hinweis, dass Daten zu Marketingzwecken gespeichert werden
- Hinweis, dass die Datenverarbeitung gemäß der gesetzlichen Bestimmungen erfolgt



- Hinweis welche welche Technologien eingesetzt werden, ( Google ads, piwik, etc)
- Angabe des Serverstandortes
- Hinweis auf Widerspruchsrecht



## Schritt 5: Brauche ich einen Datenschutzbeauftragten?

- Ja, wenn mehr als 10 Mitarbeiter ständig mit der automatisierten Datenverarbeitung personenbezogener Daten beschäftigt sind.
- „Ständig beschäftigt“ ist, wer z. B. permanent Kunden- oder Personalverwaltung macht. „Nicht“ dagegen, wer z. B. als Handwerker oder Produktionsmitarbeiter nur mit Namen und Adressen von Kunden umgeht.



# Schritt 6: Verzeichnis von Verarbeitungstätigkeiten

**Hinweis:** Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten“ gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter [www.ida.bayern.de/media/dsk\\_muster\\_yov\\_verantwortlicher.pdf](http://www.ida.bayern.de/media/dsk_muster_yov_verantwortlicher.pdf) abrufbar.

Bayerisches Landesamt für  
Datenschutzaufsicht



## Muster 3: Handwerksbetrieb – Verzeichnis von Verarbeitungstätigkeiten

### Verantwortlicher:

ABC Install GmbH  
Steinbauerstr. 45a  
98123 Sonsthausen  
Tel. 0981/123456-0  
E-Mail: team@abcinstall.de  
Web: www.abcinstall.de

Geschäftsführerin: Susanne Kühnlein, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbezogenen Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
<b>Lohn-abrechnung (über Steuerberater)</b>	Herbert Bauer 0981/123456-1 herbert@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> <li>Auszahlung der Löhne/ Gehälter</li> <li>Abfuhr Sozialabgaben u. Steuern</li> </ul>	Beschäftigte	<ul style="list-style-type: none"> <li>Name, Geburtsdatum</li> <li>Adresse</li> <li>Bankverbindungsdaten</li> <li>Lohn-/Entgelt Daten</li> <li>ggf. Religionszugehörigkeit</li> <li>Sozialversicherungsdaten</li> <li>Steuerdaten (Steuerklasse, Freibeträge,...)</li> <li>Berufsgenossenschaftsangaben</li> </ul>	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
<b>Personalverwaltung</b>	Herbert Bauer 0981/123456-1 herbert@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> <li>Personaladministration</li> <li>Personalführung</li> <li>Arbeitszeitverwaltung</li> <li>Personalbeschaffung (betrifft Bewerber)</li> </ul>	<ul style="list-style-type: none"> <li>Beschäftigte</li> <li>Auszubildende</li> <li>Bewerber</li> </ul>	<ul style="list-style-type: none"> <li>Name, Adressen</li> <li>Zeitwirtschaftsdaten</li> <li>Daten zur Arbeitsleistung</li> <li>Leistungsbeurteilung</li> <li>Lebenslauf und Bewerbungsunterlagen (betr. Bewerber)</li> </ul>	Keine	Keine	<ul style="list-style-type: none"> <li>Beschäftigte: in der Regel ca. 3 Jahre nach Ausscheiden</li> <li>abgelehnte Bewerber: 6 Monate nach Abschluss des Bewerbungsverfahrens</li> </ul>	Siehe IT-Sicherheitskonzept
<b>Betrieb der Firmenwebseite (über Hosting-Dienstleister)</b>	Max Meier 0981/123456-0 max@abcinstall.de	28.02.2018	Außerdarstellung	<ul style="list-style-type: none"> <li>Webseitenbesucher</li> </ul>	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
<b>Kundenverwaltung</b>	Janine Kleinlein 0981/123456-2 janine@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> <li>Bearbeitung von Aufträgen inkl. Rechnungsstellung</li> <li>postalische Werbung</li> </ul>	Kunden	<ul style="list-style-type: none"> <li>Name, Adresse</li> <li>Angaben zum Auftrag</li> <li>ggf. Bankverbindungsdaten</li> </ul>	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

### Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virens Scanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder





# Schritt 7: Auftragsdatenverarbeitung

- Sofern ein externer Dienstleister Daten im Auftrag eines Betriebs verarbeitet wie z.B. Buchhaltung , Hosting, Lieferant, Planer liegt eine Auftragsverarbeitung vor
- Zu diesem Zweck ist nach Art 28 DSGVO ein schriftlicher Vertrag zu schließen
- Dieser beinhaltet beispielsweise:
- Zweck und Umfang der Datenverarbeitung
- Vertraulichkeitserklärung bei der Verarbeitung von personenbezogenen Daten
- Datenverarbeitung hat auf dokumentierte Anweisung des Verantwortlichen zu erfolgen



- Festlegung der technisch organisatorischen Maßnahmen
- Kontrollrechte des Auftraggebers
- Meldung von Verstößen
- Weisungsbefugnis des Auftraggebers
  
- Wichtig: Steuerberater ist kein Auftragsdatenverarbeiter



# Schritt 8: Technisch organisatorische Maßnahmen

- Organisatorische Maßnahmen:
- Gibt es DSB?
- Wurden Mitarbeiter geschult und in das Datenschutzgeheimnis eingewiesen?
- Besteht ein Datenschutzkonzept?



- Technische Maßnahmen:
- Maßnahmen, die geeignet sind, Unbefugten den Zugang zu den Datenverarbeitungsanlagen zu verwehren
- Maßnahmen, die gewährleisten, dass Befugte nur mit Zugriffsberechtigung auf Daten zugreifen können ( Ausschluss Unberechtigter)
- Maßnahmen, die gewährleisten, dass Daten bei elektronischer Übertragung nicht von unbefugten gelesen, kopiert, verändert etc. werden können



- Maßnahmen, die gewährleisten, dass Daten nur weisungsgemäß verarbeitet werden
- Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und wann und von wem Daten eingegeben, verändert oder gelöscht wurden
- Schutz der technischen Anlagen vor zufälliger Zerstörung oder zufälligen Verlust von Daten



## Schritt 9: Meldung von Datenschutzverletzungen

- Kommt es bei der Verarbeitung von personenbezogenen Daten zu Sicherheitsvorfällen, so sind diese der Meldebehörde bekannt zu geben
- Sicherheitsvorfälle sind:
- Diebstahl, Hacking, Verlust von Tablet oder Smartphone mit unverschlüsselten Kundendaten, Fehlversendungen von Rechnungen



## Schritt 10: Löschen von Daten

- Verlangen des Kunden, dass seine Daten gelöscht werden
- Der Vertragszweck ist erreicht und es sind keine Folgeaufträge im Gespräch
- Aber: Steuerrechtliche oder handelsrechtliche Aufbewahrungsfristen sind Mindestaufbewahrungsfristen