

Karin Tausch, Sebastian Tausch



RECHT

# Datenschutz in Autohaus und Werkstatt

verstehen, umsetzen, anwenden

**asp** AUTO SERVICE PHASE BUCH **AUTOHAUS** BUCH

# Datenschutz in Autohaus und Werkstatt

Karin Tausch, Sebastian Tausch

# Datenschutz in Autohaus und Werkstatt

verstehen, umsetzen, anwenden

**Karin Tausch, Sebastian Tausch**  
Geschäftsführer und IT-Berater, IT Rechenwerk GmbH  
Hille

ISBN 978-3-574-60174-3

ISBN (eBook) 978-3-574-60175-0

© 2018 Springer Automotive Media in der Springer Fachmedien München GmbH, Aschauer Straße 30, 81549 München.

1. Auflage 2018  
Stand: Januar 2018

Produktmanagement/Lektorat: Kerstin Bandow  
Herstellung: Markus Tröger  
Satz & Layout: Schmidt Media Design, München  
Umschlaggestaltung: Bloom Project GmbH, München  
Titelbild: © weerapat1003 / stock.adobe.com  
Autorenfotos: studioline Bad Oeynhausen GmbH & Co. KG  
Druck: Bariet Ten Brink BV, Eekhorstweg 1, NL-7942 JC Meppel

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmung und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Das Werk ist mit größter Sorgfalt erarbeitet worden. Eine rechtliche Gewähr für die Richtigkeit der einzelnen Angaben kann jedoch nicht übernommen werden. Auch stellen die Informationen keine rechtliche Beratung dar und begründen somit kein Beratungsverhältnis. Die Haftung für die Inhalte der Internetverweise wird, trotz sorgfältiger inhaltlicher Überprüfung, ausgeschlossen! Für die Seiteninhalte ist ausschließlich der jeweilige Betreiber verantwortlich.

Aus Gründen der Lesbarkeit wurde im Folgenden die männliche Form (z. B. Mitarbeiter) verwendet. Alle personenbezogenen Aussagen gelten jedoch für Männer und Frauen gleichermaßen.

## Vorwort

---

Liebe Leserin, lieber Leser,

gerade Kollegen, die sich erstmalig mit dem Datenschutz befassen, können sich schnell vom Paragraphenschwungel, IT-Fachjargon und Details erschlagen fühlen. Mit unserem Buch «Datenschutz in Autohaus und Werkstatt» haben wir uns das Ziel gesetzt, Ihnen einen Routenplan an die Hand zu geben, mit dem Sie einerseits das entsprechende Grundwissen erhalten und andererseits Ihre Grunddokumentation selbstständig erstellen können.

Da wir selbst viele Jahre im Autohaus beschäftigt waren und auch heute Autohäuser und Werkstätten zu unserem Kundenkreis zählen, wissen wir, dass viele von Ihnen aufgrund der vielfältigen Tätigkeiten unter einer sehr hohen Arbeitsbelastung stehen. Deshalb liegt der Fokus dieses Buches auf der einfachen Verständlichkeit der Regelungen im Datenschutz mit Veranschaulichung anhand von praxisnahen Beispielen aus dem Autohaus und der Werkstatt.

Kurz, knapp und verständlich sorgt aber auch immer dafür, dass nicht alle Besonderheiten und möglichen individuellen Gegebenheiten vor Ort berücksichtigt werden können. Um eine möglichst hohe Übereinstimmung zu haben, gehen wir in ► Kap. 3 speziell auf besondere Verarbeitungen im Autohaus ein. Zusätzlich zu unseren eigenen Vorlagen verweisen wir zudem auch auf frei verfügbare Informationsquellen der Datenschutzaufsichtsbehörden und der Fachverbände, die gute und oftmals auch sehr umfangreiche Dokumente zur Verfügung stellen.

Einen besonderen Schwerpunkt legen wir auch auf die Datensicherheit. Denn einerseits gewinnt die sichere Verarbeitung in der Datenschutz-Grundverordnung (DS-GVO) sehr an Bedeutung und andererseits steckt hierin viel Potenzial für Ihr Autohaus. Denn immer häufiger hört man aus der Branche, dass durch diverse Angriffe versucht wird, an die Daten und/oder das Geld der Unternehmen zu gelangen. Um das Risiko zu senken, macht es deshalb Sinn, das Thema Sicherheit und die IT-Sicherheit im Speziellen ebenfalls gleich mit auf die Agenda zu setzen. Der Mehraufwand ist meistens sehr gering, da im Regelfall die gleichen Personen auf den gleichen Geräten in den gleichen Anwendungen die Daten verarbeiten.

Bitte sehen Sie das Thema Datenschutz und die dazugehörige Sicherheit nicht als ein abgeschlossenes Projekt, um Papier für die Aufsichtsbehörde zu erstellen, sondern als laufenden Prozess, der auch einen Mehrwert in Ihrem Unternehmen generieren kann. Denn einerseits haben wir eine Zeit der Rechtsunsicherheit vor uns, bis sich in der Praxis herausgestellt hat, wie bestimmte Vorschriften interpretiert werden müssen. Andererseits ändern sich laufend der Umfang der personenbezogenen Daten und die verwendete Technologie. Einige Autohäuser setzen heute schon auf Tablets, Online-

Terminbuchung, Online-Angebote für die Inzahlungnahme und den Online-Verkauf, wodurch häufig mehr personenbezogene Daten anfallen als bisher.

Abgesehen davon sammeln auch viele moderne Fahrzeuge immer mehr personenbezogene Daten. Musste man bislang eventuell nur das interne Telefonbuch und den Routenverlauf aus dem Navi löschen, sind einige Fahrzeuge heute in der Lage, ihren Zustand online an den Besitzer oder an die Werkstatt zu senden. Je digitaler das Autohaus und die internen Arbeitsprozesse werden, desto mehr muss auch der Schutz von personenbezogenen, aber auch nicht personenbezogenen Daten berücksichtigt werden.

Auch Unternehmen, die «klassisch» arbeiten, können sich der Digitalisierung kaum entziehen. Multifunktionsgeräte mit Internetanschluss statt einfacher Kopierer bzw. VoIP-Telefonie/-Anschlüsse, selbst wenn auf dem Tisch ein herkömmliches Telefon steht, sind auch hier häufig anzutreffen.

Über diese Multifunktionsgeräte werden dann die eigenen Gehaltsabrechnungen gedruckt, aber auch Personalausweise und Gehaltsnachweise von Kunden für Finanzierungsanfragen eingescannt. Werden diese Daten dann – wie bei so manchem Gerät – nach dem Druck nicht gelöscht, bleiben die Daten auf dem internen Speicher und könnten z.B. nach Rückgabe an die Leasinggesellschaft durch Dritte eingesehen werden.

Damit Sie Ihren Datenschutz im Unternehmen auch dokumentieren können, stellen wir Ihnen gerne die im Buch abgedruckten Mustervorlagen zur Verfügung. Sie sind für Sie im E-Shop unter ► [www.springer-automotive-shop.de](http://www.springer-automotive-shop.de) als kostenloser Download hinterlegt. Hierfür gehen Sie bitte auf die Artikelseite im Shop (Suche über die Bestell-Nr. 048) und klicken auf den Reiter «Downloads» unterhalb der Artikelbeschreibung. Zum Öffnen des heruntergeladenen Dokuments benötigen Sie ein Passwort, das Sie im Innenteil dieses Buches (jeweils beim Download-Hinweis der Mustervorlagen) finden.

Abschließend noch ein Tipp für AUTOHAUS-Abonnenten, der Ihnen hoffentlich viel Zeit spart. Wir durften für AUTOHAUS next ein Video für ein WBT (Web Based Training) zur ersten grundlegenden Datenschutzunterweisung der Mitarbeiter erstellen. Auf ► <https://next.autohaus.de> wird den Abonnenten dieses WBT zur Verfügung gestellt. Nach einem interaktiven Online-Training und erfolgreich bestandenen Quiz erhält jeder Teilnehmer eine Teilnahmebestätigung.

Nun bleibt uns noch, Ihnen viel Erfolg bei der Umsetzung eines effektiven und effizienten Datenschutzes in Ihrem Unternehmen zu wünschen.

Herzlichst

**Karin und Sebastian Tausch**

# Inhaltsverzeichnis

---

1	<b>Datenschutz und Datensicherheit – das steckt dahinter</b> .....	1
1.1	<b>Datenschutz und Datensicherheit</b> .....	3
1.1.1	Datenschutz versus Datensicherheit .....	5
1.1.2	Häufige Datenschutz-Pannen und Risiken .....	7
1.1.3	Die Top Ten der Datenschutzprobleme im Autohaus .....	8
1.2	<b>Die Anforderungen der neuen EU-Datenschutz-Grundverordnung</b> .....	11
1.2.1	Die Schwerpunkte: Sicherheit & Rechenschaftspflicht .....	13
1.3	<b>Die Grundprinzipien des Datenschutzes</b> .....	15
1.3.1	Die Anwendung der Grundprinzipien bei Datenschutz-Arbeiten .....	16
1.4	<b>Aufsichtsbehörden – Ratgeber &amp; Kontrolleure</b> .....	27
1.5	<b>Wer schreibt, der bleibt – die neue Relevanz technischer und organisatorischer Maßnahmen</b> .....	31
1.6	<b>So holen Sie mehr aus dem vermeintlichen «Papiertiger» für Ihr Autohaus heraus</b> ....	34
2	<b>Schritt für Schritt zur Datenschutz-Grunddokumentation</b> .....	41
2.1	<b>Datenschutz-Dokumentation</b> .....	43
2.1.1	Start: Schritt für Schritt .....	44
2.2	<b>Verantwortlichkeiten &amp; Datenschutzbeauftragter</b> .....	52
2.2.1	Wer ist eigentlich verantwortlich und welche Aufgaben hat der Datenschutzbeauftragte?	52
2.2.2	Wann muss ein Datenschutzbeauftragter benannt werden? .....	53
2.2.3	Anforderungen an den Datenschutzbeauftragten .....	54
2.2.4	Die Aufgaben des Datenschutzbeauftragten .....	57
2.2.5	Die Benennung eines Datenschutzbeauftragten .....	58
2.3	<b>Verfahrensdokumentation &amp; Verzeichnis Verarbeitungstätigkeiten erstellen</b> .....	60
2.3.1	Was ist überhaupt eine Verarbeitung? .....	61
2.3.2	Mustervorlagen und dazugehörige Informationen .....	62
2.3.3	Verzeichnis Verarbeitungstätigkeiten erstellen .....	64
2.3.4	Anwendungen erfassen .....	71
2.3.5	Technische und organisatorische Maßnahmen .....	81
2.3.6	Risikoanalyse und Datenschutz-Folgenabschätzung .....	88
2.4	<b>Mitarbeiter im Datenschutz</b> .....	97
2.4.1	Mitarbeiter-Schulung zu Beginn der Tätigkeit .....	97
2.4.2	Einwilligung zur Veröffentlichung von Bild und Kontaktdaten auf der Internetseite und im Rahmen weiterer Werbung .....	104
2.4.3	Private Nutzung geschäftlicher Dienste und Geräte sowie geschäftliche Nutzung privater Dienste und Geräte .....	108
2.5	<b>Auftragsverarbeitung</b> .....	111
2.5.1	Datenschutzkonforme Auftragsverarbeitung mit Dienstleistern .....	115
3	<b>Ein Detailblick auf wichtige Verarbeitungen im Autohaus</b> .....	121
3.1	<b>Webseite und Online-Marketing</b> .....	123

3.1.1	Die Webseite .....	123
3.1.2	Das Impressum auf der Webseite, in E-Mails und anderen Online-Präsenzen .....	130
3.1.3	Die Datenschutzerklärung auf der Webseite .....	133
3.1.4	Tipps und Tricks zum Newsletter .....	138
3.1.5	Social-Media-Anbindung und -Präsenzen .....	140
3.1.6	Datenschutz bei Werbung und Marketing .....	143
3.2	<b>Videüberwachung im Autohaus</b> .....	148
3.3	<b>Beschäftigtendatenschutz</b> .....	151
3.4	<b>Kopien von Personalausweisen und Führerscheinen</b> .....	153
3.4.1	Kopie des Personalausweises .....	153
3.4.2	Kopie des Führerscheins .....	156
3.5	<b>Cloud Computing und Schatten-IT</b> .....	157
3.5.1	Cloud Computing .....	157
3.5.2	Schatten-IT .....	160
3.6	<b>Die fachgerechte Entsorgung von Unterlagen, digitalen Datenträgern und Geräten</b> ..	161
3.6.1	Die häufig erlebte Praxis .....	161
3.6.2	Entsorgung nach DIN .....	162
3.7	<b>Datenschutz bei der Archivierung</b> .....	164
3.7.1	Verarbeitungsdokumentation & Datenkategorien .....	164
3.7.2	E-Mail-Archivierung und Datenschutz .....	166
3.8	<b>Datentransport und Verschlüsselung</b> .....	167
3.8.1	Wer hat welchen Schlüssel: symmetrisches und asymmetrisches Verfahren .....	167
3.8.2	Verschlüsselung von E-Mails .....	169
3.8.3	Verschlüsselung bei Computern, Notebooks, Smartphones, Tablets, zentralen Speichern (NAS) und Multifunktionsgeräten .....	170
3.8.4	Verschlüsselung bei mobilen Datenträgern .....	171
3.8.5	Bitte nicht vergessen: Entschlüsselung sicherstellen - auch Personalwechsel bedenken ...	171
3.9	<b>Pseudonymisierung und Anonymisierung – hier steckt Potenzial drin!</b> .....	172
3.9.1	Pseudonymisierung .....	172
3.9.2	Anonymisierung .....	174
4	<b>Wie Sie einen lebendigen Datenschutz im Autohaus etablieren</b> .....	175
4.1	<b>Wirkungsvolle Stellschrauben – in welchen wichtigen Prozessen Sie den Datenschutz verankern sollten</b> .....	177
4.2	<b>Datenschutz-Prozesse für Betroffene</b> .....	182
4.3	<b>ISO, BSI &amp; VdS – auch als Fundament für Ihre IT-Sicherheit</b> .....	191
4.4	<b>Management-Systeme verknüpfen</b> .....	194
4.5	<b>Mitarbeiter einbinden und auf dem Laufenden halten</b> .....	197
4.6	<b>Tipps &amp; Tricks zur Organisation</b> .....	201
	<b>Stichwortverzeichnis</b> .....	206





# Datenschutz und Datensicherheit – das steckt dahinter

## Zusammenfassung

Lesen Sie in diesem Kapitel, was hinter den Begriffen rund um den Datenschutz steckt und welche Pannen häufig in der Praxis anzutreffen sind. Darüber hinaus erfahren Sie, was die Anforderungen der neuen EU-Datenschutz-Grundverordnung und die Grundprinzipien des Datenschutzes sind. Außerdem lesen Sie, wie Sie mit den Aufsichtsbehörden konstruktiv zusammenarbeiten. Abgerundet wird das Kapitel von zahlreichen Beispielen und Tipps, wie Sie eine Datenschutz-Dokumentation in Angriff nehmen können und welche Vorteile ein lebendiger Datenschutz in Ihrem Betrieb hat.

- 1.1      **Datenschutz und Datensicherheit – 3**
- 1.2      **Die Anforderungen der neuen EU-Datenschutz-Grundverordnung – 11**
- 1.3      **Die Grundprinzipien des Datenschutzes – 15**

- 1.4 **Aufsichtsbehörden – Ratgeber & Kontrolleure – 27**
- 1.5 **Wer schreibt, der bleibt – die neue Relevanz technischer und organisatorischer Maßnahmen – 31**
- 1.6 **So holen Sie mehr aus dem vermeintlichen «Papiertiger» für Ihr Autohaus heraus – 34**

## 1.1 Datenschutz und Datensicherheit

Bevor wir mit der Aufnahme der Datenschutzsituation im Autohaus und der Erstellung der entsprechenden Dokumentation beginnen, sollten wir uns zuerst einen Überblick verschaffen, was sich hinter den einzelnen Begriffen Datenschutz, Datensicherheit und IT-Sicherheit verbirgt. Denn in der Praxis musste ich leider schon oft feststellen, dass diese Begriffe gerne gleichgesetzt werden oder die Unterscheidung nicht klar ist. Dies hat dann zur Folge, dass die Ziele unklar sind, die aktuelle Datenschutzsituation falsch eingeschätzt wird und schlussendlich kein wirksamer Datenschutz im Unternehmen etabliert werden kann.

### ■ Informationelle Selbstbestimmung

Um «Datenschutz» zu definieren, greifen einige Datenschutzbeauftragte auf das «Volkszählungsurteil»<sup>1</sup> des Bundesverfassungsgerichtes (BVerfG) vom 15. Dezember 1983 zurück. Dort wurde das Recht auf informationelle Selbstbestimmung aus den Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG hergeleitet. Auch wenn das Urteil schon älter ist, findet es in aktuellen Urteilen Berücksichtigung und wird zitiert. Durch die Herleitung aus dem Grundgesetz ist schön erkennbar, welchen hohen Stellenwert der Datenschutz haben sollte. Ich bevorzuge eine andere Definition, da mir diese ermöglicht neben dem Datenschutz auch die Datensicherheit und IT-Sicherheit sowie deren Verhältnis festzulegen. Dies ist insbesondere im Hinblick auf die EU-Datenschutz-Grundverordnung relevant, da mit deren Regelungen die Bedeutung der Sicherheit, insbesondere der IT-Sicherheit, stark an Bedeutung gewinnt.

### Definitionen rund um den Datenschutz

#### Datenschutz

Beim Datenschutz geht es um den Schutz personenbezogener Daten. Hierfür gibt es neben den grundsätzlichen Vorschriften, z. B. die EU-Datenschutz-Grundverordnung, zahlreiche zusätzliche Regelungen.

#### Datensicherheit

Um personenbezogene Daten zu schützen, muss eine Organisation technische und organisatorische Maßnahmen ergreifen.

#### IT-Sicherheit

Technische und organisatorische Maßnahmen für die Sicherheit von digitalen Daten werden im Rahmen der IT-Sicherheit organisiert.

#### Nicht personenbezogene Daten

Dabei sorgen Datensicherheit und IT-Sicherheit bei den meisten Unternehmen nicht nur für die Sicherheit von personenbezogenen Daten, sondern auch von nicht personenbezogenen Daten. Deshalb steigert ein Unternehmen durch einen wirksamen Datenschutz oftmals auch die gesamte Datensicherheit.

1 Volkszählungsurteil, BVerfG, 15.12.1983, ► <https://dejure.org/1983,633>

Praxisbeispiel

### Abgrenzung: Datenschutz – Datensicherheit – IT Sicherheit

**Gehaltsabrechnung** Januar 2018

Pers. Nr.	100	Abteilung	Kauf. Abt.	EV-Nummer	50000071001	Bezug. Nr. No.	
Geburtsdatum	29.03.1977	Personennummer	101	EV-Abrechnung	1.0.2018, 9.2018	Trick	Stichtag (Monat) - Kinder
EV-Bezahlung		Personennummer		EV-Bezahlung		Freibetrag	100

Herr  
 Dr. Rainer Zufall  
 Parkallee 123  
 21614 Buxtehude

EV-Tage		Su-Tage	
KE	BE	KE	BE
normal	30	30	30
normal	30	30	30
KE	1	1	1
Umsatz	0,00	Umsatz	normal
Umsatz	0,00	Umsatz	normal

Position	Bezeichnung	Monatliche Menge	Preis	Th. Bezahlung	EV	EV	EV	Bezug.
2	Gehalt				1	1	2	3.300,00 EUR

Datenschutz

Datensicherheit

IT-Sicherheit

Abb. 1.1 Beispiel personenbezogene Daten Gehaltsabrechnung (Quelle: eigene Darstellung)

Lassen Sie uns das Beispiel in Abb. 1.1 etwas ausführlicher ansehen. Es zeigt eine Gehaltsabrechnung, die eine hohe Anzahl an personenbezogenen Daten enthält, beispielsweise Name, private Anschrift, Bankverbindung etc. Somit müssen die Vorschriften des Datenschutzes eingehalten werden.

**Punkt 1:** Diese Vorschriften besagen z. B., dass Ihr Autohaus nur die Daten von den Mitarbeitern verarbeiten darf, welche unbedingt für den Zweck – z. B. Gehaltsabrechnung – erforderlich sind. Zudem muss diese Verarbeitung auch dokumentiert werden, wie wir auch in den nachfolgenden Kapiteln sehen werden.

**Punkt 2:** Im Rahmen der Dokumentation müssen wir auch festlegen, welche Maßnahmen zur Datensicherheit durchgeführt werden. Sehr wahrscheinlich haben Sie dafür schon einige Maßnahmen, welche bislang vermutlich noch nicht dokumentiert werden. So werden die Gehaltsabrechnungen sicherlich nicht offen im Pausenraum zur Mitnahme ausgelegt, sondern in einem verschlossenen Kuvert übergeben oder verschickt. Zudem werden Papierausdrucke sehr wahrscheinlich sicher verwahrt, z. B. in verschlossenen Schränken oder Büros, so dass kein Unbefugter diese einsehen kann.

**Punkt 3:** Sofern die Gehaltsabrechnungen im Autohaus eigenständig durchgeführt werden, erfolgt dies sicherlich über eine entsprechende Software. In diesem Fall ist es sehr wahrscheinlich, dass sowohl der Computer als auch die Gehalts-Software abgesichert sind, also z. B. ein Zugriff nur mit Benutzername und Passwort möglich ist und die Daten regelmäßig gesichert werden. Werden die Gehaltsabrechnungen von einem Dienstleister oder dem Steuerberater erstellt, wurden auch hier sicherlich technische und organisatorische Maßnahmen der IT-Sicherheit festgelegt, damit kein Unbefugter diese einsehen kann, z. B. eine gesicherte Übertragung der Daten eingerichtet.

## 2.1.1 Start: Schritt für Schritt

Gemeinsam gehen wir in diesem Kapitel Schritt für Schritt die Erstellung der Datenschutz-Grunddokumentation durch. Natürlich variiert der Weg je nach Betrieb immer etwas. Im einen Fall sind Sie vielleicht selbst für die IT verantwortlich und müssen nicht auf die Rückmeldungen Ihrer Kollegen oder Mitarbeiter warten. In einem anderen Fall haben Sie vielleicht keinen Verkauf oder keinen Werkstattbereich. Aus diesem Grund möchte ich an dieser Stelle nochmals speziell darauf hinweisen, dass es sich bei dem Ablauf um einen Vorschlag handelt und bei den abgebildeten Formularen um Muster, die Sie an Ihre Bedürfnisse anpassen sollten. Ich verweise alternativ auch an geeigneter Stelle auf Vorlagen, Muster und Checklisten der Aufsichtsbehörden oder Verbände. Damit haben Sie einerseits eine größere Auswahl und – wie z. B. bei den Vorlagen zur Auftragsverarbeitung – den Vorteil, dass eine größere Anzahl an Fachleuten diese so sicher wie möglich gestalten und bei Bedarf auch sicherlich aktualisieren.

### Tipp

Achten Sie bei Ihren Anpassungen immer darauf, dass einerseits die ggf. vorgeschriebenen Pflichtinformationen enthalten sind und andererseits, dass die Angaben so detailliert und transparent wie möglich sind. Es ist auch nicht grundsätzlich verboten, in den eigenen, internen Unterlagen weiterführende Informationen zu vermerken.

### Schritt 1: Ordner oder Verzeichnisse anlegen

In einem ersten Schritt empfiehlt es sich die Grundstruktur der späteren Dokumentation anzulegen. Dies hat den Vorteil, dass Sie Informationen, Checklisten, Ideen und Ähnliches im Laufe Ihrer Datenschutz-Arbeit ablegen und bei Bedarf schnell wieder darauf zugreifen können. Ob Sie die Dokumentation und dazugehörigen Informationen in Papierform oder digital verwalten, bleibt Ihrer Arbeitsweise überlassen. Ich gehe in der Beschreibung von der Papierform aus.

In der Praxis hat es sich als vorteilhaft herausgestellt, einen Ordner mit der grundsätzlichen Dokumentation zu verwenden und laufende Arbeiten in einem oder später dann mehreren Arbeitsordnern abzulegen. Da alle wesentlichen Informationen im Grundordner zu finden sind, hilft er dabei den Überblick zu behalten – sowohl für die eigene Arbeit als auch für Kollegen, die eventuell darauf zugreifen müssen, oder Dritte, die berechtigt Einblick nehmen wollen.

Nachfolgend beschreiben wir den Aufbau der Ordner und stellen kurz den jeweiligen Inhalt vor. Auf die weiteren Details, also im Regelfall die Inhalte der einzelnen Register, werden wir in den späteren Abschnitten und Kapiteln genauer eingehen.

## ■ Ordner 1: Grunddokumentation

### ■ ■ Register 1: Informationen zum Unternehmen

Im ersten Ordner sollten sich Informationen zum Unternehmen befinden. Diese Informationen sollten einem Dritten einen Überblick ermöglichen, wie das Unternehmen strukturiert ist und wer für welche Bereiche Verantwortung trägt. Sehr gut eignen sich hierfür z. B. Organigramme, aus denen hervorgeht, welche Sparten und Abteilungen es gibt und wer jeweils verantwortlich ist.

Auch wenn Ihr Betrieb kleiner ist und keine Abteilungen und Abteilungsleiter hat, sollten Sie dort zumindest Informationen hinterlegen, wer für welche Arbeiten zuständig ist. Übliche Arbeiten sind z. B. IT/EDV, Personalverwaltung, Buchhaltung, Verkauf, Werkstatt und ggf. der Handel mit Teilen. Damit kann ein Dritter, z. B. ein Mitarbeiter einer Aufsichtsbehörde, sich schnell einen Eindruck verschaffen, wie das Unternehmen organisiert ist.

Wenn Sie Organigramme haben, sollten Sie nicht vergessen den Datenschutzbeauftragten darin zu vermerken – und zwar direkt unterhalb der obersten Unternehmensleitung, wie dies in Art. 38 Abs. 3 der Datenschutz-Grundverordnung vorgesehen ist.

### ■ ■ Register 2: datenschutzrelevante Prozesse

Vermutlich wird die erste Anfrage eines Betroffenen eintreffen, wenn Sie sich gerade in den verdienten Urlaub verabschiedet haben oder aufgrund anderer Arbeiten überhaupt keinen Kopf dafür haben. Auch wird die Aufregung groß sein, wenn es zu einem Datenschutzvorfall kommt und in dieser Ausnahmesituation unklar ist, ob nun gemäß Art. 33 Abs. 1 der Datenschutz-Grundverordnung eine Meldung innerhalb von 72 Stunden an die Aufsichtsbehörde erfolgen muss.

In diesem Fall ist es sehr hilfreich, wenn Ihre Kollegen oder auch Sie selbst vorab überlegt haben, wie vorzugehen ist. Dafür eignen sich Ablaufpläne oder Prozessbeschreibungen, aus denen z. B. ersichtlich ist, ob der Vorfall unter die Meldepflicht fällt oder nicht und im schlimmsten Fall wer, in welcher Form und mit welchen Angaben die Meldung durchführt bzw. wer die Entscheidung trifft und wer im Vorfeld informiert werden sollte.

#### Tipp

Mein Tipp ist, sich gerade am Anfang nicht zu sehr mit der Optik des Dokuments aufzuhalten, sondern lieber vorhandene Muster anzupassen oder per Hand den möglichen Ablauf zu skizzieren. Im Laufe der Erstellung der Datenschutz-Grunddokumentation wird es immer wieder Anpassungsbedarf in den Dokumenten geben. In der Praxis kann ein entsprechender Vermerk in dieser Form schneller erfolgen als ein aufwendig gestaltetes Dokument anpassen zu müssen. Der Form halber sollten Sie aber das jeweilige Datum und den Verfasser notieren und bei Anpassungen eine vorher erstellte Kopie des alten Standes aufbewahren.

### Checkliste Newsletter

Die Verarbeitung «Newsletter» sollte in der Datenschutz-Dokumentation dokumentiert werden.	
Sofern ein E-Mail-Newsletter-Anbieter zum Einsatz kommt, sollte geprüft werden, ob ein Vertrag zur Auftragsverarbeitung erforderlich ist und dieser entsprechend abgeschlossen werden.	
Es sollte regelmäßig geprüft werden, ob alle erforderlichen Pflichtangaben im Anmeldeformular (ggf. Print und online) und in den eigentlichen Newslettern bzw. Vorlagen enthalten sind.	

## 3.1.5 Social-Media-Anbindung und -Präsenzen

Gerade die großen und bekannten sozialen Netzwerke wie Facebook, Google (YouTube, Google+) und dazugehörigen Kommunikationsanbieter wie WhatsApp (Facebook) sind bei den Aufsichtsbehörden alles andere als beliebt. Dementsprechend schwierig – wenn nicht gar unmöglich – ist es auch, dort datenschutzkonform präsent zu sein. Da die meisten uns bekannten Autohäuser dort aber mit einer Fanpage vertreten sind, möchten wir im Folgenden die wichtigsten Punkte aufzählen. Auf Details wie z. B. Werbeanzeigen oder «Facebook Pixel» gehen wir nicht ein. Einerseits, weil es für die wenigsten Leser interessant sein dürfte und andererseits, weil sich die Anforderungen und Möglichkeiten sehr schnell ändern.

### Tipp

Auf der Webseite der Bayerischen Aufsichtsbehörde (► [www.lida.bayern.de](http://www.lida.bayern.de)) finden Sie hierzu aber recht umfangreiche Informationen.

### ■ Die wichtigsten Punkte bei einer Präsenz in sozialen Netzwerken

#### ■ ■ Punkt 1: immer ein aktuelles und leicht erreichbares Impressum

Wie auch bei der Webseite sollten Sie stets darauf achten, ein aktuelles und leicht erreichbares Impressum bereitzuhalten. Je nach Anbieter kann dies über eine eigene Seite erfolgen oder notfalls auch per Link zum Impressum Ihrer Webseite. Notfalls deshalb, weil es hier passieren kann, dass sich ggf. der Link des Impressums ändert oder die Seite – aus technischen Gründen – nicht erreichbar ist, womit dann kein Impressum zur Verfügung steht.

#### ■ ■ Punkt 2: nicht den Zugriff verlieren

Nicht selten betreuen Mitarbeiter, die auf den Plattformen auch selbst privat aktiv sind, die Präsenz des Autohauses. Was auf den ersten Blick ganz praktisch ist, birgt zwei große Risiken. Risiko 1 ist, dass ein Mitarbeiter, häufig auch Azubi, das Autohaus verlässt und mit ihm auch der Zugriff auf die eigene Präsenz verloren geht. Hier sollten Sie unbedingt darauf achten, dass der Zugriff weiterhin gewahrt bleibt und den Zugriff am besten über ein separates oder über mehrere Konten ermöglichen.

## 3.2 Videoüberwachung im Autohaus

Die EU-Datenschutz-Grundverordnung selbst enthält, im Gegensatz zum neuen Bundesdatenschutzgesetz, keine spezifischen Regelungen zur Videoüberwachung. Ob die Regelungen des neuen Bundesdatenschutzgesetzes allerdings zur Anwendung kommen, ist noch unklar, da die EU-Datenschutz-Grundverordnung Vorrang hat. Damit bleibt die Videoüberwachung wie bisher ein «heißes Eisen» und muss sorgfältig betrachtet werden. Da wir in diesem Abschnitt nur auf die wichtigsten Punkte zum Thema Videoüberwachung eingehen, möchten wir an dieser Stelle auf eine Orientierungshilfe der Aufsichtsbehörden verweisen. Diese wurde zwar für das bisherige Bundesdatenschutzgesetz erstellt, zeigt aber an vielen Stellen die Ansicht der Aufsichtsbehörden zu Detailfragen, die bisher auch nicht gesetzlich geregelt waren.

### Tip

Sie finden die Orientierungshilfe unter ► <https://www.bfdi.bund.de/> im Menü Infothek /Entschlüsselungen und hier im Unterpunkt «Entschlüsselungen des Düsseldorfer Kreises».

### ■ Rechtliche Grundlage für eine Videoüberwachung nach EU-Datenschutz-Grundverordnung

In den meisten Fällen dürfte für Autohäuser wohl Art. 6 Abs. 1 S. 1 lit. f die passendste Rechtsgrundlage sein:

- » ...die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Allerdings birgt diese Rechtsgrundlage eine große Gefahr: Sie ist so vage, dass sie – zumindest auf den ersten Blick – eigentlich für alle Verarbeitungen zum Einsatz kommen könnte, wenn sich nicht ein anderes Gesetz findet. Deshalb sollten Sie bei den anderen erforderlichen Angaben selbst mit strengem Blick prüfen, ob die Videoüberwachung wirklich diesen Zweck erfüllt, ob die Speicherdauer – ggf. auch für einzelne Kameras – nicht auch kürzer sein könnte oder die Überwachung vielleicht auch nur zu bestimmten Zeiten, z. B. nach Geschäftsschluss, ausreichend ist.

### ■ Achten Sie auf eine genaue Zweckbestimmung!

«Mit den Videokameras schützen wir unser Gebäude und unsere Waren» ist die übliche Antwort auf die Frage nach dem Zweck einer Videoüberwachungsanlage. Das ist allgemein verständlich, aber leider nicht konkret und «wahr» genug. Denn eine Videoüberwachungsanlage, die lediglich aufzeichnet, «schützt» ja nicht konkret vor einem Einbruch, sondern die Aufzeichnungen helfen – nach Weitergabe der Daten an Dritte – bei der



keine Vereinbarungen getroffen hat. Hinzu kommt, dass die meisten Anbieter ihren Sitz in einem sogenannten Drittland haben und somit oftmals personenbezogene Daten ohne Einwilligung der Betroffenen dorthin transferiert werden.

#### Tipp

Kurzum: Fragen Sie Ihre Mitarbeiter oder Kollegen, ob diese (personenbezogene) Daten auf privaten Geräten oder privaten Online-Anwendungen verarbeiten. Erfragen Sie bitte insbesondere die Nutzung von WhatsApp auf dem geschäftlichen Smartphone oder die geschäftliche Nutzung von WhatsApp auf dem privaten Smartphone. Sofern dies der Fall ist und tatsächlich Bedarf besteht, sollten Sie datenschutzkonforme Alternativen suchen. Das können u. U. sogar die gleichen Anbieter bleiben, nur eben mit geschäftlichem Konto und datenschutzkonformen Vereinbarungen. Es gibt zahlreiche datenschutzfreundliche Alternativen, die zum Einsatz kommen können. Selbst der Einsatz von WhatsApp lässt sich dank spezieller Apps häufig realisieren.

## 3.6 Die fachgerechte Entsorgung von Unterlagen, digitalen Datenträgern und Geräten

---

Nach einigen Themen, bei denen noch vieles unklar ist, kommen wir nun zu einem Thema, bei dem wir uns sogar auf DIN-Normen berufen können: die korrekte Löschung vor Weitergabe oder Entsorgung.

### 3.6.1 Die häufig erlebte Praxis

---

In Autohäusern und Werkstätten werden relativ viele und teilweise auch sensible Daten verarbeitet. Interessenten und Kunden bringen Ihre Gehaltsabrechnungen für Finanzierungsanfragen mit und Personalausweise werden für Probefahrten, größere Barzahlungen, Finanzierungen, Zulassung und Bestellung diebstahlrelevanter Teile kopiert. Manchmal wird die Sensibilität der Daten auch erst auf den zweiten Blick erkennbar, z. B. wenn Fehldrucke von Werkstattaufträgen oder Rechnungen komplett lesbar im Papierkorb landen und einem Dritten in die Hände fallen. Mag sein, dass es bei einem Großteil der Kunden keine Auswirkungen hat, wohl aber wenn der aufgedruckte Empfänger ein Prominenter ist oder andere Begehrlichkeiten weckt. Nicht selten finden wir bei unseren Bestandsaufnahmen neben komplett lesebaren Auftrags- oder Rechnungsdokumenten die bereits erwähnten Personalausweiskopien und Gehaltsabrechnungen im Altpapier.

Noch riskanter wird es natürlich, wenn digitale Datenträger wie Festplatten, CDs, DVDs, USB-Sticks etc. ohne – korrekte – Löschung entsorgt werden. Gleiches gilt für Geräte, in denen entsprechende Speicher eingebaut sind, also Server, Computer, Tablets, Smartphones, Multifunktionsgeräte etc.