Leitfaden

Datenschutz-Grundverordnung (DSGVO)

VERLÄSSLICH
IST MODERN TAXI

Die Inhalte dieses Leitfadens basieren auf der Broschüre „Erste Hilfe zur Datenschutz-Grundverordnung“, herausgegeben vom Bayerischen Landesamt für Datenschutzaufsicht. Er stellt eine stark reduzierte Zusammenfassung von deren Inhalt dar, die mit Beispielen (auch aus anderen Quellen) angereichert wurde. Eine rechtlich abschließende und verbindliche Beratung kann dieser Leitfaden nicht leisten. Für spezielle Einzelfragen zu individuellen Situationen des Betriebes sollten entsprechende Experten hinzugezogen werden.
Zur vertieften Befassung können wir die Broschüre „Erste Hilfe zur Datenschutz-Grundverordnung“ nur bestens empfehlen (C.H. Beck-Verlag, ISBN 978-3-406-71662-1, Preis 5,50 €)**.**

Inhaltsverzeichnis **Seite**

Kapitel 1: Anwendungsbereich der DSGVO

Die Europäische Datenschutz-Grundverordnung (DSGVO) gilt als Europäische Verordnung seit dem 25. Mai 2018 unmittelbar in allen EU-Mitgliedsstaaten und bedarf keiner weiteren nationalen Umsetzung mehr. Auch das nationale Recht in Gestalt des Bundesdatenschutzgesetzes (BDSG) wurde angepasst (= BDSG (neu)) und enthält teilweise die DSGVO ergänzende Regelungen. Es ersetzt das bisherige BDSG und ist ebenfalls zum 25. Mai 2018 in Kraft getreten.

Die DSGVO gilt für die komplett oder teilweise automatisierte **Verarbeitung personenbezogener Daten** sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Dies sind nicht zwangsläufig digitale Daten, auch ein nach bestimmten Kriterien geordneter Karteikasten aus Papier kann bereits den Anwendungsbereich der DSGVO eröffnen.

Definition: Personenbezogene Daten sind alle Informationen und Angaben, die sich einer bestimmten **natürlichen Person** (also einem Menschen) zuordnen lassen und sie dadurch identifizieren oder identifizierbar machen kann (vgl. Art. 4 Abs. 1 DSGVO, Bsp.: Namen, Online-Kennung, Wohnort, Steuernummer, Religionszugehörigkeit etc.).

Das **Verarbeiten** ist dabei ein umfassender Begriff für den Umgang mit personenbezogenen Daten und umfasst z. B. das Erheben, Speichern, Ändern, Übermitteln oder auch Löschen von Daten. **Jeder Umgang mit personenbezogenen Daten ist damit als Verarbeiten im Sinne der DSGVO zu betrachten.** Die Verarbeitung von personenbezogenen Daten für ausschließlich persönliche und familiäre Tätigkeiten (z. B. Adressbücher oder Fotos) fällt aber nicht in den Anwendungsbereich der DSGVO.

Wer Dienstleistungen oder Waren in Deutschland beziehungsweise der EU anbietet und Mitarbeiter in seinem Unternehmen beschäftigt, ist bereits **Verarbeiter** und muss die DSGVO anwenden.

Wer darüber hinaus in fremden Namen (also im Auftrag eines Dritten) Dienstleistungen oder Waren in Deutschland beziehungsweise der EU anbietet, ist bereits ein sogenannter **Auftragsverarbeiter** und muss insofern auch die entsprechenden Vorschriften der DSGVO beachten.

Kapitel 2: Erste Schritte

Nachdem Sie vermutlich mit Schrecken festgestellt haben, dass auch für Sie beziehungsweise Ihren Betrieb die DSGVO einschlägig ist, gilt es, sich mit der Umsetzung der neuen gesetzlichen Anforderungen auseinanderzusetzen. Viele der Pflichten sind für deutsche Unternehmen gar nicht so neu, da sie bereits im (alten) BDSG bestanden haben. Angesichts der aktuell hohen Aufmerksamkeit für das neue Datenschutzrecht und auch im Hinblick auf die sehr empfindlichen Sanktionsandrohungen (bis zu 20.000.000 Euro oder bis zu 4 % des gesamten weltweiten Jahresumsatzes) ist aber jeder Unternehmer angehalten, sich mit der Problematik auseinanderzusetzen!

Hierzu empfiehlt sich allgemein folgende Vorgehensweise:

1. Machen Sie sich bewusst, dass Datenschutz Chefsache ist und gegebenenfalls nicht kostenlos zu haben ist.

2. Verschaffen Sie sich einen – aus datenschutzrechtlicher Sicht – Überblick, was Sie in Ihrem Unternehmen machen in Gestalt eines **Verzeichnisses von Verarbeitungstätigkeiten**. Dies ist praktisch unabdingbare Pflichtübung für jedes Unternehmen!
3. Überprüfen Sie, ob Sie zur Erfüllung Ihrer Aufgaben andere Unternehmen als **Auftragsdatenverarbeiter** (z.B. bei Krankenfahrten-Abrechnungen!) eingeschaltet haben und falls ja, ob Sie mit diesen die für die Verarbeitung personenbezogener Daten erforderlichen Verträge abgeschlossen haben.
4. Machen Sie sich bewusst, dass sowohl Mitarbeiter als auch Kunden und Fahrgäste, deren Daten Sie erhoben und gespeichert haben, sogenannte **Betroffenenrechte** geltend machen können. Diese müssten gegebenenfalls in kurzer Zeit vollständig und richtig erfüllt werden können.
5. Prüfen Sie, ob die Verarbeitung personenbezogener Daten in Ihrem Unternehmen datenschutzrechtlich zulässig ist und Sie diese Zulässigkeit auch jeweils nachweisen können.
6. Last but not least, prüfen Sie, ob Sie einen Datenschutzbeauftragten bestellen müssen.

Definition: Verzeichnis von Verarbeitungstätigkeiten ist das Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten. Dieses Verzeichnis betrifft sämtliche – auch teilweise – automatisierte Verarbeitungen, ferner nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Siehe Checkliste für die ersten Schritte zur Einhaltung der DSGVO, Anlage 1!
In Anlage 1a) finden Sie eine spezielle „kleine Checkliste“ für Taxiunternehmen.

Kapitel 3: Verarbeitungsverzeichnis

Grundsätzlich müssen nach Art. 30 DSGVO alle Verantwortlichen (= Jeder, der mit personenbezogenen Daten von anderen umgeht) ein Verzeichnis über alle Verarbeitungsprozesse erstellen und fortführen. Zwar gibt es eine theoretische Freistellung von dieser Verpflichtung für Unternehmern und Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen. Dies ist in der Praxis aber bedeutungslos, da die Freistellung nur dann gilt, wenn die Verarbeitung nur gelegentlich erfolgt und keine Verarbeitung besonderer Datenkategorien nach Art. 9 DSGVO wie Gesundheits- oder Religionsdaten erfolgt. Damit sind nach strenger Auslegung bereits Unternehmen, die kontinuierlich Lohnabrechnungen einschließlich der Verarbeitung von Religionsdaten zur Abrechnungen von Kirchensteuern durchführen, betroffen. Erst recht aber der Taxiunternehmer mit Krankenfahrten und entsprechender Verarbeitung besonders sensibler Gesundheitsdaten!

Deshalb ist anzuraten, im Zweifel lieber ein Verzeichnis der Verarbeitungstätigkeiten aufzustellen. Es hilft zudem jedem Verantwortlichen, einen Überblick über den Umgang mit personenbezogenen Daten zu erlangen. Das Verzeichnis kann auch im Hinblick auf die Erfüllung weiterer gesetzlich verpflichtender Aufgaben notwendig sein.

Die Verzeichnisse sind regelmäßig in deutscher Sprache zu führen und können schriftlich oder auch elektronisch vorgehalten werden. Sind nicht öffentlich und dienen neben der eigenen Qualitätskontrolle ausschließlich für den Nachweis gegenüber der Aufsichtsbehörde, in welchem Verfahren in dem jeweiligen Unternehmen mit personenbezogenen Daten umgegangen wird. Die Verzeichnisse müssen immer aktuell sein und mindestens die in Art. 30 Abs. 1 DSGVO genannten Bestandteile beinhalten:

- Name und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorie personenbezogener Daten
- Kategorien von Empfängern von Daten einschließlich Empfänger in Drittstaaten
- wenn möglich, vorgesehene Löschungsfristen
- wenn möglich, eine Beschreibung der technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus (gem. Artikel 32 Abs 1 DSGVO)

Insbesondere bei größeren Unternehmen und komplexeren Verarbeitungstätigkeiten empfiehlt sich ein sogenanntes **erweitertes Verzeichnis**, mit dem **konkrete Verarbeitungstätigkeiten** im Sinne der Definition im Art. 4 Nr. 2 DSGVO (erheben, speichern, abfragen, offenlegen usw.) beschrieben und die **herangezogenen Rechtsgrundlagen** aufgeführt werden (z. B. Art. 6 DSGVO, Arbeitsvertrag, Betriebsvereinbarungen, Einwilligung usw.). Durch ein erweitertes Verzeichnis kann jeder sehr schnell für sich selbst und auch im Fall der Prüfung durch die Aufsichtsbehörde Rechenschaft darüber ablegen, ob die Datenverarbeitung zulässig ist.

Siehe anliegendes Muster eines Verzeichnisses von Verarbeitungstätigkeiten, Anlage 2.
Als Anlage 2a) finden Sie das Musterbeispiel eines Verarbeitungsverzeichnisses für ein Taxiunternehmen.

Kapitel 4: Grundsätze für die Verarbeitung personenbezogener Daten

1. Verbot mit Erlaubnisvorbehalt

Im Datenschutzrecht gibt das sogenannte Prinzip des **Verbots mit Erlaubnisvorbehalt**. Grundsätzlich gilt also ein Verbot für die Verarbeitung von personenbezogenen Daten. Nur bei Vorliegen einer gesetzlich festgelegten Ausnahme (vgl. Art. 6 DSGVO) dürfen Daten überhaupt erhoben und verarbeitet werden, nämlich wenn:

- die betroffene Person eine **Einwilligung** erteilt hat; oder
- die Verarbeitung für die **Erfüllung eines Vertrages** oder einer rechtlichen Verpflichtung erforderlich ist; oder
- die Verarbeitung zur **Wahrung von berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich ist und nicht den Interessen der betroffenen Personen überwiegend entgegenstehen.

Wenn man danach Daten verarbeiten darf, muss sichergestellt sein, dass dabei insbesondere die **Zweckbindung**, **Richtigkeit** und **Erforderlichkeit** beachtet werden und nicht zuletzt darüber Rechenschaft abgelegt werden kann. Näheres im Folgenden:

2. Rechtmäßigkeit

Wichtig ist, dass vor dem Umgang mit personenbezogenen Daten geprüft wird, ob eine Rechtsgrundlage hierfür besteht. Eine Verarbeitung ohne Rechtsgrundlage ist unzulässig und kann zu hohen Bußgeldern führen.

a) Einwilligung

Art. 4 Nr. 11 DSGVO **definiert die Einwilligung** als jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Einwilligungen sind nach Art. 7 DSGVO (vgl. auch § 51 BDSG (neu)) deshalb nur dann wirksam, wenn

- sie freiwillig abgegeben werden,
- sie für einen bestimmten Fall abgegeben werden (eine pauschale Einwilligung zu allen heute und in Zukunft relevanten Zwecken ist zu unbestimmt und damit wohl ungültig),
- die betroffene Person klar und verständlich informiert wurde, für welchen Zweck die Daten verarbeitet werden sollen,
- die betroffene Person darüber informiert wurde, dass sie die Einwilligung jederzeit (ohne Angabe eines Grundes) widerrufen kann,
- die Einwilligung schließlich durch eine eindeutig bestätigende Handlung erfolgt (z. B. schriftliche Erklärung, aktives Ankreuzen einer Erklärung im Internet, sog. "opt-in", das „Stehenlassen" eines bereits vorangehakten Kästchens („opt-out") reicht nicht).

Anmerkung: einen Mustertext für eine Einwilligungserklärung zur Datenverarbeitung bei Krankenfahrten sowie weitere Hinweise finden Sie in Anlage 3.

b) Vertragserfüllung

Personenbezogene Daten, die zur Erfüllung eines Vertrages notwendig sind, dürfen verarbeitet werden.

c) Wahrung berechtigter Interessen des Verantwortlichen

Personenbezogene Daten dürfen auch „zur Wahrung berechtigter Interessen des Verantwortlichen verarbeitet werden, sofern nicht die Interessen der betroffenen Personen überwiegen". Bei der Interessenabwägung ist auf die „vernünftige Erwartung einer betroffenen Person" abzustellen. Auch wenn diese Rechtsgrundlage die unbestimmteste und am schwierigsten nachzuweisende ist, wird sie wohl diejenige sein, auf die die meisten Datenverarbeitungen gestützt werden!

Weiter muss nicht nur eine der Rechtsgrundlagen (a bis c) vorliegen, sondern es müssen zudem noch die folgenden Grundsätze beachtet werden:

3. Zweckbindung

Eine Verarbeitung personenbezogener Daten – egal, ob auf der Basis einer Einwilligung, eines Vertrages oder einer Interessenabwägung – darf nur für die konkreten, vorab festgelegten Zwecke erfolgen.

Tipp: Befassen sie sich damit, was jeweils als Zweck für Ihre Datenverarbeitung verstanden werden soll. Prüfen Sie, ob und welchen Zweck Sie den betroffenen Personen genannt haben. Stellen Sie sicher, dass die Daten auch nur für diesen Zweck verwendet werden.

4. Datenrichtigkeit

In der DSGVO ist ausdrücklich geregelt, dass die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen. Die Aktualität der Daten muss deshalb mit angemessenem Aufwand sichergestellt werden.

Beispiel: Bei Namensänderung durch Heirat bei einem Verbandsmitglied müssen die Verantwortlichen sicherstellen, dass der Name an allen relevanten Speicherorten geändert wird.

5. Erforderlichkeit der Speicherung

Die Verantwortlichen dürfen nur diejenigen personenbezogenen Daten erheben und speichern, die für die Erreichung des o. g. zulässigen Zwecks erforderlich sind.

Hier muss beachtet werden, dass personenbezogene Daten, die für den Zweck nicht mehr erforderlich sind und für die es keine sonstigen Aufbewahrungsvorschriften (z.B. steuerliche oder handelsrechtliche Aufzeichnungspflichten, Auftragseingangsbuch für Mietwagenunternehmen nach § 49 Absatz 4 PBefG) mehr gibt, entweder zu löschen oder aber so zu ändern sind, dass jeglicher Personenbezug wegfällt.

6. Dokumentations- und Rechenschaftspflicht

Mit der Rechenschaftspflicht besteht für die Verantwortlichen eine neue und erhebliche Herausforderung. Die o.g. datenschutzrechtlichen Grundsätze müssten nicht nur eingehalten werden, sondern deren Einhaltung z. B. gegenüber der Aufsichtsbehörde auch nachgewiesen werden können!

Konkret bedeutet dies, dass eine Aufsichtsbehörde von dem Verantwortlichen verlangen kann, dass er im Zweifel durch Vorlage einer schriftlichen Dokumentation nachweisen kann, welche personenbezogenen Daten von Mitarbeitern, Kunden, Lieferanten oder Vereinsmitgliedern er verarbeitet. Weiter muss er nachweisen, auf welcher Rechtsgrundlage dies konkret geschieht, für welchen Zweck die Daten verwendet werden und wie lange sie gespeichert werden sollen.

Diese Verpflichtung trifft nicht nur große Unternehmen, sondern alle!

Nach § 29 DSGVO dürfen die dem Verantwortlichen unterstellten Personen mit Zugang zu personenbezogenen Daten diese ausschließlich auf Weisung des Verantwortlichen verarbeiten. **Für den Verantwortlichen ist es deshalb geboten, die Mitarbeiter auf eine gesetzeskonforme und weisungsgemäße Verarbeitung der ihnen anvertrauten und zugänglichen personenbezogenen Daten schriftlich (Nachweisbarkeit!) zu verpflichten.** Hier ist im Zweifel im Arbeitsvertrag oder als Ergänzung zu diesem zu einer entsprechenden schriftlichen Aufklärung anzuraten, die vom Mitarbeiter durch Unterschrift bestätigt wird.

Tipp: Die im Mai 2018 aktualisierten **Muster-Arbeitsverträge des BZP** enthalten eine solche Verpflichtung auf das Datengeheimnis, bei bestehenden Arbeitsverhältnissen kann mit einer separaten Erklärung gearbeitet werden. Auch hierfür gibt es eine vom BZP erarbeitete Vorlage – unbedingt vom Arbeitnehmer unterschreiben lassen!

Siehe Anlage 4: Muster Verpflichtung auf das Datengeheimnis

Die Rechenschaftspflicht kann insbesondere bei Kleinunternehmen relativ leicht durch ein „**erweitertes Bearbeitungsverzeichnis**“ (mit über den Mindestinhalt hinausgehenden Beschreibungen

der konkreten Verarbeitungstätigkeit und Benennung der herangezogenen Rechtsgrundlage für die Verarbeitung) erfüllt werden.

Wer dagegen in Bezug auf die Rechenschaftspflicht weder eine schriftliche noch eine elektronische Dokumentation vorweisen kann, kann nicht unerhebliche Probleme bekommen.

Kapitel 5: Auftragsverarbeitung

Häufig schalten Unternehmer externe Dienstleister ein, die für das Unternehmen z. B. die IT-Einrichtung warten, Buchhaltung erledigen oder die Lohn- und Gehaltsabrechnung übernehmen. Ein klassisches Beispiel im Taxi- und Mietwagengewerbe ist die Abrechnung von Krankenfahrten durch externe Dienstleister wie Abrechnungszentren.

Wenn diese Dienstleister bei derartigen Aufgaben für andere bei der Erfüllung mit personenbezogenen Daten umgehen, spricht man von einer Auftragsverarbeitung. Die Auftragsverarbeitung wird hauptsächlich in Art. 28 DSGVO geregelt.

Definition: Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.

Der Verantwortliche gibt also personenbezogene Daten an jemanden außerhalb seines Unternehmens (z. B. Mitarbeiterdaten an eine externe Buchhaltung) oder er ermöglicht den Einblick auf die eigene Daten (Wartung der eigenen IT durch eine externe Firma). „Im Auftrag“ bedeutet, dass allein das Unternehmen über Zwecke und Mittel der Verarbeitung entscheidet, das heißt, der Auftragsverarbeiter weisungsabhängig den Auftrag erfüllt („verlängerte Werkbank“). Das liegt z. B. vor bei datenverarbeitungstechnischen Arbeiten für die Lohn- und Gehaltsabrechnungen.

Keine Auftragsverarbeitungen sollen dagegen vorliegen, wenn externe Beratungs- und Dienstleistungen in Anspruch genommen werden (z. B. Wirtschaftsprüfung, Steuerberatung, Inkassotätigkeit mit Forderungsübertragung).

Bei der Auftragsdatenverarbeitung wird keine ausdrückliche Einwilligung der betroffenen Personen oder eine sonstige gesetzliche Grundlage für die Weitergabe der personenbezogenen Daten benötigt.

Wer einen Auftragsverarbeiter einschalten möchte, muss aber vorher prüfen, ob dieser hinreichend Garantie dafür bietet, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften erfolgt. Für die Auftragsdatenverarbeitung ist ein Vertrag zwischen dem Unternehmen (Verantwortlicher) und dem Auftragsverarbeiter zu schließen, der die datenschutzrechtlichen Pflichten des Auftragsverarbeiters festlegt und das Weisungsrecht des Verantwortlichen festschreibt. Der Auftraggeber muss sich bei dem Auftragsverarbeiter dabei umfangreiche Kontrollrechte zur Überprüfung der Einhaltung der Pflichten des Auftragsverarbeiters vorbehalten. Auch müssen in dem Vertrag bereits entsprechende Regelungen für das Ende der Vertragsbeziehung getroffen werden (was ist zurückzugeben, zu löschen bzw. zu vernichten).

Kapitel 6: Sicherheit der Verarbeitung

Cyberangriffe und Hacker-Attacken können mittlerweile jeden treffen, dabei können sensible Daten wie Kreditkartendaten, Email-Adressen samt Passwörtern oder auch Gesundheitsdaten abgegriffen werden. Die DSGVO legt deshalb besonderes Augenmerk auf die Sicherheit der Verarbeitung

personenbezogener Daten, konkrete Anforderungen werden in Art. 32 DSGVO geregelt. Danach sind unter Berücksichtigung des Stands der Technik, der Kosten und des Risikos der Datenverarbeitung unter anderem folgende Maßnahmen notwendig:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit** und Belastbarkeit der Systeme sicherzustellen,
c) die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) regelmäßig die technischen und organisatorischen Maßnahmen zur Sicherheitsgewährleistung zu überprüfen, zu bewerten und gegebenenfalls zu verbessern.

Bei dem Schutzziel **Vertraulichkeit** geht es darum, Informationen vor Unbefugten zu verbergen. Beispiel: Bei **Datenfunkdisplays** könnten andere Fahrgäste ggf. Namen und Adressen anderer Taxibesteller einsehen. Hier wird angeraten, mit sogenannten **Blickschutzfolien** zu arbeiten.

Unter **Integrität** soll die Unversehrtheit von Informationen sichergestellt werden. Hieran fehlt es, wenn Daten beabsichtigt oder unbeabsichtigt manipuliert (also verändert) werden.

Mit dem Ziel **Verfügbarkeit** soll dafür gesorgt werden, dass die vorhandenen Daten bei Bedarf jederzeit genutzt werden können.

Entsprechende Maßnahmen zu IT-Sicherheit sind also nicht nur eine unverbindliche Empfehlung, sondern eine rechtliche Pflicht, der sich die Verantwortlichen bewusst sein müssen. Auch die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten können erforderliche Sicherheitsmaßnahmen sein.

IT-Sicherheit ist deshalb Chefsache. Selbst bei kleineren Unternehmen macht es folglich Sinn, IT-Sicherheitsrichtlinien zu erstellen, die die wesentlichen Aspekte für den eigenen sicheren Betrieb umschreiben. Trotz schriftlicher Dokumentation von Sicherheitsmaßnahmen wie z. B. durch Passwortrichtlinien ist natürlich die gelebte Praxis entscheidend. Deshalb wird auch für Betriebe mit einer größeren Anzahl von Mitarbeitern empfohlen, einen **IT-Sicherheitsbeauftragten** zu benennen.

Zu Sicherheitsrichtlinien gehört auch ein **Berechtigungsmanagement**, Art. 32 Abs. 4 DSGVO erwähnt explizit, dass die internen Abläufe im Betrieb so organisiert sein müssen, dass es auch dort nicht zu Sicherheitsverletzungen kommt. Also muss festgelegt werden, wer auf welche Daten für welchen Zweck in den jeweiligen Systemen zugreifen darf. Ein gut gepflegtes Berechtigungsmanagement gilt deshalb als A und O eines guten Sicherheitskonzeptes, dabei sollten jeweils nur die absolut erforderlichen Rechte erteilt werden. Bei ausscheidenden Mitarbeitern ist zu gewährleisten, dass die Zugriffrechte vollständig entzogen werden.

Explizit wird auch **Verschlüsselung** als geeignete Maßnahme zur Sicherheit der Verarbeitung in Art. 32 Abs. 1a DSGVO aufgeführt. Hier bestehen häufig Berührungsängste, obwohl Verschlüsselungsverfahren in der heutigen Praxis häufig schon benutzt werden, wenn auch unbewusst.

So ermöglicht die Einstellung „**STARTTLS“ bei Email-Servern** eine **durchgängige Transportverschlüsselung** nach dem Stand der Technik. Wenn sie für ihre E-Mail-Kommunikation einen deutschen Provider nutzen, können sie davon ausgehen, dass diese Option vorhanden ist.

Wenn Sie einen eigenen E-Mail-Server betreiben, müssen Sie darauf achten, dass Ihr IT-Dienstleister diese Einstellungen vornimmt.

Sobald personenbezogene Daten auf einer **Webseite** verarbeiten werden, ist **HTTPS** als Transportverschlüsselung eine erforderliche Sicherheitsmaßnahme!

Bei **WLAN-Netzen**, die für eigene Unternehmenszwecke oder auch für Gäste zur Verfügung gestellt werden, ist zwingend auf ausreichenden Schutz vor unbefugten Zugriffen zu achten. So ist das WLAN-Netz selbst als auch der Zugriff auf den WLAN-Router durch ein **ausreichend sicheres Passwort** zu verhindern. Voreingestellte Passwörter zur Konfiguration von WLAN-Routern sollten umgehend geändert werden!

Allgemein ist beim Umgang mit **Soft- oder Hardware** zu berücksichtigen, dass es immer **Sicherheitslücken** geben wird. Weitverbreitete Systeme wie beispielsweise Content-Management-Systeme für Webseiten sind ein beliebtes Angriffsziel. Man sollte sich deshalb regelmäßig über Sicherheitslücken erkundigen und Herstellerhinweise verfolgen („**Patch-Management“**).

Wegen der zunehmenden Verbreitung von Schadcodes, z. B. sogenannter Erpressersoftware (Computer wird durch Schadcodes gesperrt und nur gegen ein Lösegeld wieder freigegeben) werden dringend vorbeugende **Backups** als zentrale Sicherheitsmaßnahme empfohlen. Diese sollten regelmäßig durchgeführt und auf Medien gespeichert werden, die nicht mit dem eigentlichen Firmennetz verbunden sind. Der **wichtigste Schutz** gegen solche Schadsoftware oder sonstige Angriffe von außen stellt aber die **fachkundige Unterrichtung und Sensibilisierung** der **Mitarbeiter** eines Betriebes dar. Die Schadcodes infiltrieren die Firmen fast ausschließlich über E-Mail-Anhänge, infizierte Webseiten oder befallene Datenträger. Mitarbeiter sollten geschult werden, sogenannte Phishing-Nachrichten zu erkennen und ausführbare Dateianhänge in E-Mails von unbekannten Absendern nicht zu öffnen.

Last but not least sollten Unternehmen auch ausreichende Schutzmaßnahmen ergreifen, dass die eigenen **Geschäftsräume physikalisch** vor **dem Zutritt von Unbekannten geschützt** sind.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt auf seiner Internetseite typische Irrtümer zur IT-Sicherheit vor. Diese sollten beachtet werden, bevor man sich selbst in falscher Sicherheit wiegt und daraus Schäden entstehen. Link:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Sicherheitsirrtuemer/Sicherheitsirrtuemer.html?cms_pos=1

Exkurs: Datenschutzfolgeabschätzung

Art. 35 DSGVO fordert eine **Datenschutzfolgeabschätzung**, wenn ein Verfahren voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen birgt. Dies ist bei besonders sensiblen Daten wie zum Beispiel Gesundheitsdaten naheliegend. So können Krankentransportverordnungen auf dem Postweg verloren gehen, an die falsche Mailadresse übermittelt werden oder auch offen im Fahrzeug liegend von nicht autorisierten Personen eingesehen werden. Für solche Fälle ist eine Datenschutzfolgeabschätzung zwingend notwendig.

Als erster Schritt ist zu prüfen, ob ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Wird ein solches Risiko bejaht, muss überprüft werden, ob die Sicherheitsvorkehrungen zum Schutz der Daten ausreichend sind. Es muss ein Nachweis erfolgen, dass die DSGVO eingehalten und die Interessen der Betroffenen beachtet wurden.

Kommt der Unternehmer zu dem Ergebnis, dass trotz aller Maßnahmen das Risiko gleichwohl hoch bleibt, muss eine Meldung an die Aufsichtsbehörde erfolgen (Art. 36 DSGVO).

Kapitel 7: Datenschutzbeauftragter

Unter bestimmten Voraussetzungen muss ein Datenschutzbeauftragter (=DSB) benannt werden. Der DSB soll den bzw. die Verantwortlichen und die Beschäftigten über die Datenschutzvorschriften unterrichten und sie beratend fachlich unterstützen. Er soll die Einhaltung der Datenschutzvorschriften überwachen und die Selbstkontrolle des Unternehmens oder des Vereins beim Datenschutz unterstützen. Der DSB soll mit der Aufsichtsbehörde zusammenarbeiten und für diese Anlaufstelle in Fragen sein, die mit der Verarbeitung personenbezogener Daten zusammenhängen. Wann ein DSB bestellt werden muss, erläutert übersichtsweise der Fragenkatalog auf Seite 12.

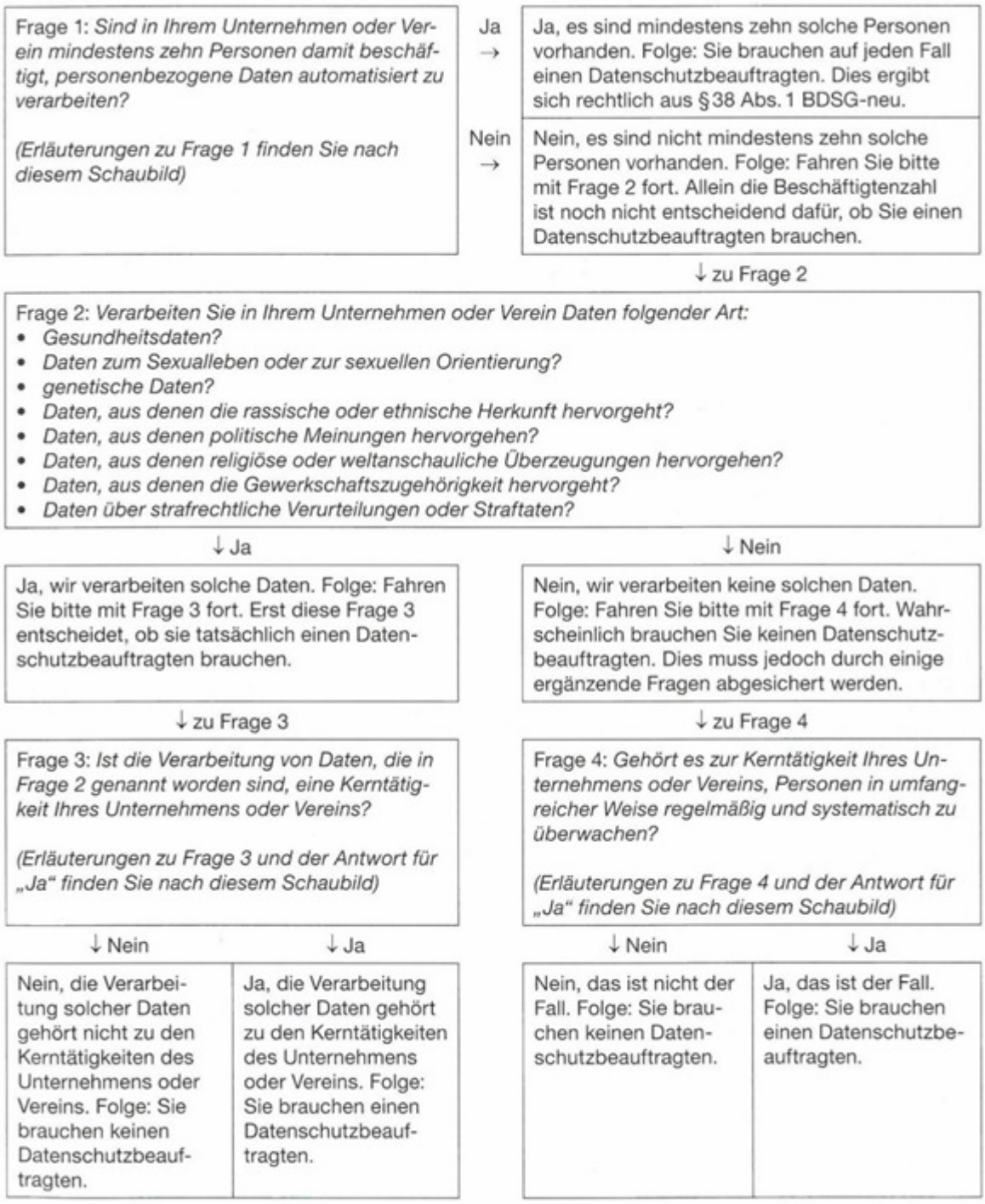
Erläuterung zum Fragenkatalog: Nach Art. 37 DSGVO i.V.m. § 38 BDSG (neu) ist ein Datenschutzbeauftragter **zwingend** zu ernennen, wenn **mindestens 10 Personen ständig damit beschäftigt sind**, personenbezogene Daten automatisiert zu verarbeiten. Dabei wird auf die Kopfanzahl abgestellt, auch Teilzeitbeschäftigte zählen voll! Als automatisierte Verarbeitung sind z.B. PC-Arbeitsplätze in der Disposition anzusehen.

Weiter ist nach Art. 37 DSGVO ein DSB (auch bei kleineren Unternehmen!) zwingend zu ernennen, wenn die **Kerntätigkeit des Unternehmens** in der **umfangreichen Verarbeitung besonders schutzwürdiger Personendaten** besteht. Zu den besonders schutzwürdigen Personendaten zählen:

- Gesundheitsdaten
- Daten zum Sexualleben oder zur sexuellen Orientierung
- Genetische Daten
- Daten, aus denen die rassische oder ethnische Herkunft hervorgeht
- Daten, aus denen die politischen Meinungen hervorgehen
- Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen
- Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht
- Daten über strafrechtliche Verurteilungen oder Straftaten.

Im Taxi- und Mietwagengewerbe werden im Bereich der Krankenfahrten besonders **Gesundheitsdaten** verarbeitet. Dies führt aber nur dann zur Notwendigkeit eines Datenschutzbeauftragten, wenn die Verarbeitung der Gesundheitsdaten zur **Kerntätigkeit** des Unternehmens gehört. Nur wenn diese Frage ebenfalls bejaht wird, ist zwangsläufig auch bei Kleinunternehmen die Bestellung eines Datenschutzbeauftragten notwendig.

Fragenkatalog: Muss ein Datenschutzbeauftragter bestellt werden?



Die Verarbeitung bestimmter Daten gehört dann zur Kerntätigkeit eines Unternehmens oder Vereins, wenn der Zweck des Unternehmens oder Vereins sonst nicht erreicht werden könnte. Beispiel: Ein Unternehmen, das individuell angepasste medizinische Hilfsmittel für Kunden herstellt, kann diese Tätigkeit nur ausüben, wenn es über die entsprechenden Gesundheitsdaten der Kunden verfügt. Dann muss z. B. auch ein Hörgeräteakustiker mit lediglich zwei Mitarbeitern zwingend einen Datenschutzbeauftragten benennen, da die Verarbeitung der Gesundheitsdaten zur Kerntätigkeit seines Unternehmens gehört.

Nach unserer Einschätzung ist dies bei professionellen Abrechnungsdiensten oder ggf. auch Taxizentralen mit einer professionalisierten Krankenfahrten-Abrechnung der Fall, nicht dagegen jedoch bei kleineren Unternehmen, die ihre selbst durchgeführten Krankenfahrten abrechnen. Allerdings bestehen hier noch ziemliche Unsicherheiten. So sieht der bayerische Landesdatenschutz z. B. keine zwingende Bestellung eines Datenschutzbeauftragten bei Arztpraxen trotz der dort verarbeiteten Gesundheitsdaten, eine ähnliche Einschätzung besteht auch in Baden-Württemberg.

Wir raten deshalb, im Zweifel gegebenenfalls über Ihren Landesverband eine Anfrage an den zuständigen Landesdatenschutzbeauftragten zu stellen!

Weiter sieht Art. 37 DSGVO auch die Benennung eines Datenschutzbeauftragten vor, wenn die Kerntätigkeit des Unternehmens in der umfangreichen und systematischen Überwachung von Personen besteht.

Darüber hinaus besteht immer auch die Möglichkeit, einen Datenschutzbeauftragten **freiwillig** zu benennen. Dies kann allein schon vor dem Hintergrund sinnvoll sein, dass die Verantwortung für die Einhaltung der Vorschriften auf jeden Fall den Verantwortlichen (also die Unternehmensleitung oder den Vereinsvorsitzenden) trifft und es ihm häufig an der erforderlichen fachlichen Unterstützung fehlt.

Grundsätzlich können **interne** (also ein Mitarbeiter des Betriebs) oder **externe Datenschutzbeauftragte** benannt werden. Auf jeden Fall muss der Datenschutzbeauftragte aber fachliche Qualifikationen auf dem Gebiet des Datenschutzes besitzen (IT-Fachwissen und Datenschutzrecht), es darf auch kein Interessenkonflikt zu sonstigen (grundsätzlich aber möglichen) Tätigkeiten im Unternehmen bestehen.

Interner vs. externer Datenschutzbeauftragter:

- Ein interner DSB darf wegen der Erfüllung seiner Aufgaben weder abberufen noch benachteiligt werden. Für seine zusätzliche Funktion als DSB sind ihm die notwendige Zeit und Unterstützung (z.B. Fortbildung, Ausstattung) zu geben. Ein interner DSB unterliegt zudem einem besonderen Kündigungsschutz: Das Arbeitsverhältnis darf während der Tätigkeit als DSB und für ein Jahr danach nicht gekündigt werden, es sei denn, die Kündigung erfolgt aus wichtigem Grund (fristlose Kündigung).

- Ein externer DSB gehört nicht dem Betrieb an. Infolgedessen gelten für ihn die besonderen Kündigungsschutzregeln nicht. Zudem kann der Dienstleistungsvertrag mit einem externen DSB grundsätzlich jederzeit gekündigt werden, soweit vertraglich nicht etwas anderes vereinbart wird.

Auch wenn nicht ausdrücklich vorgeschrieben, wird dringend empfohlen, die Benennung des Datenschutzbeauftragten schriftlich durchzuführen, **siehe hierzu das Muster als Anlage 5!**

Ein DSB ist bei seiner Aufgabenerfüllung weisungsunabhängig, jedoch nicht weisungsbefugt. Er berichtet unmittelbar der Geschäftsführung und ist bei allen datenschutzrechtlichen Themen frühzeitig einzubinden.

Zwingend muss der Verantwortliche die **Kontaktdaten des Datenschutzbeauftragten der Aufsichtsbehörde mitteilen** (Art. 37 Abs. 7 DSGVO). Hierfür stehen in der Regel Online-Formulare bei den Aufsichtsbehörden zur Verfügung.

Weiter sieht das Gesetz auch vor, dass die **Kontaktdaten des Datenschutzbeauftragten veröffentlicht** werden. Sinnvoll ist eine Veröffentlichung im Internet, wobei Namen oder gerade die persönliche Anschrift veröffentlicht werden müssen, vielmehr genügt eine E-Mail-Funktionsadresse (z.B. Datenschutzbeauftragter@abc.de). Es muss aber sichergestellt sein, dass Nachrichteneingänge unter dieser Adresse regelmäßig abgerufen werden und diese auch nur vom DSB oder einer von ihm autorisierten Person gelesen werden können.

Kapitel 8: Betroffenenrechte

Die DSGVO schützt die Rechte und Freiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten durch sogenannte **Betroffenenrechte**. Durch diese sollen die Betroffenen die Möglichkeit der Kenntnisnahme erhalten, wer welche Informationen über sie zu welchem Zweck gespeichert hat und wie er sie nutzt.

Hierdurch werden Unternehmen verpflichtet, aktiv im Wege einer transparenten Information über die von ihnen geplante Datenverarbeitung zu informieren. Andererseits müssen Anforderungen Betroffener auf Auskunft, Berechtigung, Löschung, Einschränkung der Verarbeitung, Übertragung der Daten, Widerspruch gegen die Verarbeitung und das Recht nicht ausschließlich Objekt eines Computerprogrammes zu sein, unverzüglich erfüllt werden können! Die Betroffenenrechte sind in den Art. 12 bis 23 der DSGVO geregelt und werden durch die §§ 32 bis 37 BDSG (neu) ergänzt. Die Betroffenenrechte im Einzelnen:

1. Transparente Information

Bei jedem Umgang mit personenbezogenen Daten sind die Personen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache **unverzüglich vor (!) Verwendung der Daten zu informieren**. Konkret muss insbesondere informiert werden über:

- Namen und Kontaktdaten des Verantwortlichen
- Kontaktdaten eines Datenschutzbeauftragten (sofern vorhanden),
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und die Rechtsgrundlagen dafür
- Interessen des Verantwortlichen, wenn Daten auf der Basis einer Interessensabwägung verarbeiten möchten
- Empfänger der Daten, wenn der Verantwortliche sie weitergeben möchte

Ferner müssen Verantwortliche den betroffenen Personen unter anderem auch folgende, nach der DSGVO erforderlichen Informationen zur Verfügung stellen (vergleiche auch Artikel 13 DSGVO):

- Dauer der Speicherung der Daten oder Kriterien für die Löschung
- Hinweis auf Recht auf Auskunft, Berichtigung, Löschung etc.
- Hinweis, dass eine Einwilligung jederzeit grundlos widerrufen kann und
- Hinweis auf Beschwerderecht bei der Aufsichtsbehörde.

2. Auskunftsrecht

Das Recht auf Auskunft nach Art. 15 DSGVO ist an sich nichts Neues. Betroffene können eine Bestätigung verlangen, ob über sie personenbezogene Daten gespeichert und verarbeitet werden. Eine Auskunft ist nicht automatisch zu erteilen, sondern nur auf konkreten Antrag hin. Dabei ist

wichtig, dass man sich darüber vergewissert, dass der Antragsteller auch derjenige ist, der er zu sein vorgibt. Nur bei hinreichender Sicherheit hierüber darf die entsprechende Auskunft erteilt werden. Auch wenn man keine Daten von derjenigen Person hat, ist man dennoch verpflichtet, dies dem Antragsteller mitzuteilen. Sofern man aber personenbezogene Daten vom Antragsteller gespeichert hat, muss man ihm diese als Abschrift (als schriftliche oder elektronische Zusammenfassung) zukommen lassen. Insbesondere sind folgende Informationen mitzuteilen:

- Zweck der Verarbeitung
- Kategorie personenbezogener Daten
- Empfänger der Daten
- Geplante Speicherdauer
- Hinweis auf sonstige betroffene Rechte und Beschwerdemöglichkeiten bei der Aufsichtsbehörde

Die Auskunft muss der Verantwortliche **kostenlos zur Verfügung stellen** und dabei auch das Porto selbst tragen.

3. Berichtigung, Löschung und Einschränkung der Verarbeitung (Artikel 16-18 DSGVO)

Sind personenbezogene Daten falsch, nicht mehr aktuell oder vollständig, haben die betroffenen Personen nach Artikel 16 DSGVO ein Recht auf unverzügliche **Berichtigung**. Der **Anspruch auf Löschung** muss erfüllt werden, wenn eine der Löschungsgründe des Artikels 17 DSGVO vorliegt. Dies ist der Fall, wenn die Aufbewahrung der Daten für die Erfüllung des ursprünglichen Zwecks nicht mehr erforderlich ist, die Daten unrechtmäßig verarbeitet worden sind, der Betroffene seine Einwilligung für eine weitere Speicherung widerrufen hat und es keine andere Rechtsgrundlage für die weitere Speicherung der Daten gibt. Man spricht in diesem Zusammenhang auch vom „**Recht auf Vergessenwerden**“.

Sofern die Richtigkeit der gespeicherten Daten streitig ist, hat die betroffene Person einen **Anspruch auf Einschränkung der Verarbeitung** (Artikel 18 DSGVO). Der Verantwortliche darf die Daten dann zwar noch speichern, aber nicht mehr in sonstiger Art und Weise verarbeiten, also bspw. einem Dritten übermitteln oder für Werbezwecke nutzen.

4. Pflicht zur Datenübertragung

Das Recht auf Datenübertragung gibt Betroffenen unter bestimmten Voraussetzungen den Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen Dateiformat zu erhalten, vgl. Art. 20 DSGVO.

Der Betroffene hat damit das Recht, Daten von einem Anbieter zu einem anderen Anbieter mitzunehmen (Beispiel: Online-Shop). Die Regelung soll den Anbieterwechsel insbesondere bei sozialen Netzwerken oder Verträgen mit Banken, Energieversorgern und Versicherungen erleichtern. Dies betrifft allerdings nur die Daten, die die betroffene Person selbst übermittelt hat und nicht etwa Erkenntnisse, die der Verantwortlicher aus ihnen gezogen hat (z. B. Nutzerverhalten, Vorlieben).

5. Widerspruch gegen die Verarbeitung

Den Betroffenen steht ein Widerspruchsrecht gegen eine Verarbeitung ihrer Daten zum Zwecke der Direktwerbung zu. Die Nutzung der Daten zur Direktwerbung ist weiterhin zulässig, betroffene

Personen können jedoch jederzeit und ohne Angaben von Gründen widersprechen. Der Verantwortliche ist dann immer verpflichtet, in Zukunft auf Werbemaßnahmen zu verzichten.

6. Recht, keinen automatisierten Entscheidungen unterworfen zu werden

Durch dieses Recht hat der Betroffene in aller Regel einen Anspruch darauf, dass nicht ein Computer alleine darüber entscheidet, wie mit seinen personenbezogenen Daten umgegangen wird bzw. Konsequenzen aus der Verarbeitung gezogen werden. Ausnahmen hiervon bestehen, wenn die betroffene Person ausdrücklich eingewilligt hat oder die Verarbeitung auf Grundlage einer Rechtsvorschrift erfolgt.

In kleinen Unternehmen dürfte dieser Fall aber nur sehr geringe Bedeutung haben, da hier ganz überwiegend individuelle Kommunikation stattfindet.

7. Zwischenfazit: Vorbereiten!

Die umfangreichen Betroffenenrechte sind nicht leicht zu erfüllen. Zudem müssen diese nach Artikel 12 DSGVO unverzüglich erfüllt werden können, also spätestens nach einem Monat. Es ist deshalb für alle Verantwortlichen notwendig, sich auf die evtl. Inanspruchnahme o.g. Rechte vorzubereiten. Hierzu ist z.B. ein vollständiges und aktuelles **Verzeichnis der Verarbeitungstätigkeiten** äußerst hilfreich. Hierdurch können Daten schnell und vollständig zusammengeführt werden und eine vollständige Auskunft erteilt werden.

ACHTUNG: Wenn Sie diesen Betroffenenrechten nicht zeitnah nachkommen und die Betroffenen sich bei der Aufsichtsbehörde beschweren, haben sich mit nicht unerheblichen Bußgeldern zu rechnen! Seien Sie also vorbereitet!

Kapitel 9: Verletzung des Schutzes personenbezogener Daten

Bei einer Verletzung des Schutzes personenbezogener Daten (siehe nachfolgende Definition) muss der Verantwortliche diese im Normalfall unaufgefordert innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde melden, Artikel 33 Abs. 1 Satz 1 DSGVO, ansonsten kann ein erhebliches Bußgeld drohen.

Definition: Die **Verletzung des Schutzes personenbezogener Daten** ist eine Verletzung der Sicherheit, die unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Der Begriff „Verletzung des Schutzes personenbezogener Daten“ bezeichnet

- Jede Verletzung der Sicherheit
- in Bezug auf personenbezogene Daten,
- die eine negative Konsequenz hinsichtlich dieser Daten haben kann

Als negative Konsequenzen hinsichtlich der Daten sind denkbar:

- Vernichtung der Daten (= die Daten existieren nicht mehr)
- Verlust der Daten (= die Daten existieren zwar noch irgendwo, sind aber für den Verantwortlichen nicht mehr greifbar)
- Veränderung der Daten (= die Daten sind inhaltlich nicht mehr zuverlässig)

- Unbefugte Offenlegung der Daten (= die Daten sind nicht mehr geschützt und Personen, denen diese Daten gar nichts angehen, können sie möglicherweise zur Kenntnis nehmen)
- Unbefugter Zugang zu den Daten (= Unbefugte haben Zugriff auf die Daten erhalten)

Unerheblich ist, um welche Art von Daten es sich handelt, so lange sie personenbezogen sind. Es muss sich also nicht um besonders sensible Daten im Sinne von Artikel 9 DSGVO (z.B. Gesundheitsdaten) handeln. Auch ist unerheblich, ob die Datenpanne absichtlich oder unbeabsichtigt erfolgt ist. Eine Verletzung bedeutet nicht zwangsläufig, dass es zu einem Schaden für die betroffenen Personen kommen wird oder kann.

Rechtsfolge ist die Meldepflicht. Die Meldepflicht nach Artikel 33 Abs. 1 Satz 1 DSGVO an die Aufsichtsbehörde besteht unverzüglich und entfällt nur dann, wenn die Schutzverletzung voraussichtlich zu keinem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dies dürfte in der Praxis nur selten vorliegen. „Unverzüglich“ bedeutet, dass der Verantwortliche ohne schuldhaftes Zögern handeln muss. Er darf also zunächst durchaus versuchen, den Sachverhalt aufzuklären. Aber: Die Meldepflicht besteht bereits dann, wenn erste belastbaren Informationen vorliegen. Es ist nicht notwendig, dass die Informationen bereits vollständig sind. Dabei sind alle Fakten, die im Zusammenhang mit einer Schutzverletzung stehen, **genau zu dokumentieren,** Artikel 33 Abs. 5 Satz 1 DSGVO. Die Meldung an die Aufsichtsbehörde ist „möglichst binnen 72 Stunden“ nach Bekanntwerden der Verletzung zu erbringen. Wird diese Frist überschritten, ist dies zu begründen. Der Inhalt einer solchen Meldung ist im Artikel 33 Abs. 2 DSGVO detailliert vorgeschrieben.

Sofern für die betroffenen Personen die Schutzverletzung „voraussichtlich **ein hohes Risiko für die persönlichen Rechte und Freiheiten**“ zur Folge hat, sind die **betroffenen Personen zwingend zu benachrichtigen**. Die betroffenen Personen müssen nur dann nicht benachrichtigt werden, wenn geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen wurden (Artikel 34 Abs. 2 Satz 1a DSGVO). Wichtigste Maßnahme ist eine ausreichende Verschlüsselung aller personenbezogenen Daten, die eine Kenntnisnahme durch Unbefugte verhindert.

TIPP Zum Thema Verschlüsselung auf mobilen Geräten, PC´s wie auch Verschlüsselung der Kommunikation gibt es eine gut verständliche Anleitung beim Bundesamt für Sicherheit in der Informationstechnik (BSI). LINK:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesselung_node.html

Sofern die **Benachrichtigung** von **betroffenen Personen** erfolgen muss, ist zunächst festzustellen, welche Personen im Einzelnen betroffen sind. Hierfür ist das Verzeichnis der Verarbeitungstätigkeiten hilfreich (siehe auch Kapitel 3). Aus diesem müsste sich zumindest eine abstrakte Beschreibung des Personenkreises der Betroffenen ergeben. Die Information selber muss „**in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten**“ beschreiben, siehe Artikel 34 Abs. 2 DSGVO. Ferner muss die Information folgende Angaben enthalten:

- Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen.
- Eine Beschreibung der wahrscheinlichen Folgen der Schutzverletzung

- Eine Beschreibung der vom Verantwortlichen ergriffenen oder von ihm vorgeschlagene Maßnahme zur Behebung der Schutzverletzung bzw. Maßnahmen zur Abmeldung der nachteiligen Auswirkungen der Schutzverletzung

Beispiel einer Betroffenen-Benachrichtigung:

Daten über Ihre bei unserer Firma getätigte Bestellung mitsamt Ihren Kontonummern wurden auf dem Laptop Ihres persönlichen Kundenbetreuers gespeichert. Dieser wurde bei einer Bahnreise im Zug gestohlen. Unbefugte könnten die Bestellscheine und die Rechnungen zu Ihren Bestellungen lesen und die darin enthaltenen Daten einschließlich Kontonummern entnehmen. Soweit Bestellscheine und Rechnungsangaben zu Ihrer Kontoverbindung enthalten sind, sollten Sie in nächster Zeit regelmäßig überprüfen, ob es zu verdächtigen Transaktionen auf Ihrem Konto kommt.

Kapitel 10: Sanktionen und Haftung

Durch die Datenschutzgrundverordnung und das neu gefasste Bundesdatenschutzgesetz (BDSG (neu)) wurden die bisher geltenden Regelungen deutlich verschärft, Verstöße gegen den Datenschutz können ernsthafte rechtliche Folgen nach sich ziehen. So sieht Artikel 83 DSGVO Geldbußen von bis zu 20 Mio. Euro oder bis zu vier Prozent des weltweit erzielten Gesamtumsatzes vor, im Extremfall sogar bis zu 40 Mio. Euro. Damit sollen gegenüber Großunternehmen wie Facebook und Co. auch wirklich spürbare Sanktionen möglich sein. Aber auch bei kleinen und mittleren Unternehmen ist mit erheblichen Geldbußen zu rechnen, denn die Geldbußen müssen „in jeden vereinzelten Fall wirksam, verhältnismäßig und abschreckend“ sein, vergleiche Artikel 83 Abs. 1 DSGVO sowie die korrespondierenden nationalen Vorschriften der §§ 42 und 43 BDSG (neu). Für den vorsätzlichen unbefugten gewerbsmäßigen Handel mit personenbezogenen Daten stehen sogar Strafandrohungen von bis zu drei Jahren Freiheitsstrafe, vergleiche § 42 Abs. 1BDSG (neu).

Aber auch leichte Verstöße können empfindliche Sanktionen nach sich ziehen, typische Beispiele hierfür:

- Versendung von E-Mails mit offenem Verteiler, so dass jeder Empfänger ohne einen sachlichen Grund auch alle anderen Empfänger sehen kann
- Aushang von Krankheitslisten von Mitarbeitern am „schwarzen Brett“
- Wiederholte Faxsendungen mit medizinischen Daten an falsche Empfänger

Zudem hat jede Person Anspruch auf Schadensersatz, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Artikel 82 Abs. 1 DSGVO.

Kapitel 11: Anforderungen an die eigene Unternehmensstruktur

Nach der DSGVO müssen die Verantwortlichen Rechenschaft über den Umgang mit personenbezogenen Daten ablegen können. Im Unternehmen oder Verein muss jemand konkret bestimmt sein, der im Zweifel den Kopf dafür hinhalten muss. Ansprechpartner für die Aufsichtsbehörde ist im Unternehmen oder Verein grundsätzlich die Unternehmensleitung bzw. der Vorstand. **Datenschutz ist damit Chefsache.** Das bedeutet nicht, dass der Chef sich persönlich um die Einhaltung der Datenschutzvorschriften kümmern muss, er muss aber die Verantwortlichkeiten regeln.

Ein evtl. **eingesetzter Datenschutzbeauftragter** ist aber für die Umsetzung nicht verantwortlich! Die Aufgabe des DSB ist, wie bereits im Kapitel 7 ausgeführt, zu kontrollieren, zu beraten und darauf hinzuwirken, dass die Regeln des Datenschutzes auch beachtet werden. Verantwortlich selbst ist der Chef oder die von ihm beauftragte Person.

Diese muss im Zweifel sicherstellen, dass ein Verzeichnis der Verarbeitungstätigkeiten erstellt wird, Mitarbeiter in Datenschutzfragen geschult werden, das Unternehmen bzw. der Verein auf Anfragen von betroffenen Personen zeitnah reagieren kann und – last but not least – Datenschutzverletzungen erkannt und ggf. auch gemeldet werden.

Weiter empfiehlt es sich, einen **Überprüfungszyklus für Datenschutzfragen** festzulegen. Auch wenn es naheliegt, die Anforderungen der DSGVO zeitnah nach Inkrafttreten am 25.05.2018 zu prüfen, hat die Erstprüfung keinen ewigen Bestand. Es wird deshalb allgemein empfohlen, einen Überprüfungszyklus festzulegen, innerhalb dessen z.B. das Verzeichnis der Verarbeitungstätigkeiten überprüft, Mitarbeiterschulungen wiederholt oder regelmäßigen „Trockenübungen“ für die Erfüllung von Betroffenenrechten oder die Meldung von Datenschutzverletzung erfolgen.

Ein entsprechendes, kurzes Manual kann Klarheit schaffen.

Tipp: Allgemein gilt, dass die Erfüllung möglichst vieler Anforderungen wie z.B. vorliegende und gepflegte Verzeichnisse der Verarbeitungstätigkeiten und schriftlich festgelegte Überprüfungszyklen für die Sorgfalt des Unternehmens im Umgang mit persönlichen Daten sprechen und bei evtl. Verstößen gegenüber der Behörde ein positiveres Gesamtbild des Unternehmens vermitteln!

Kapitel 12: Umgang mit der Aufsichtsbehörde

Den **Datenschutzaufsichtsbehörden** wurden durch die DSGVO nicht nur Kontrollaufgaben und Sanktionsbefugnisse übertragen. Sie haben auch die **Aufgabe, Betroffene und Verantwortliche** zu **beraten**, wie die Anforderungen der DSGVO erfüllt werden können.

Haben Sie also keine Scheu, sich in Zweifelsfragen an Ihre zuständige Aufsichtsbehörde zu wenden! Dies kann auch für typisierte Problemfälle des Gewerbes sinnvoller Weise durch den Landesverband erfolgen. Die Erfahrungen zeigen, dass die Rechtsauslegungen in Zweifelsfragen von Land zu Land durchaus variieren können. Da sowohl die Europäische Datenschutzverordnung als auch die nationale Umsetzung durch das neue BDSG viele Neuregelungen enthalten, gibt es noch keine gefestigte Rechtsprechung dazu. Ein Grund mehr, in Zweifelsfragen die für Sie zuständige Behörde einzubinden.

Auch wenn die Anzahl der Beschäftigten in den Aufsichtsbehörden im Verhältnis zu dem Wust der Aufgaben gering erscheinen mag, sollte mit der Einhaltung der Vorschriften nicht lässig umgegangen werden. Bereits eine Beschwerde eines unzufriedenen Mitarbeiters, Kunden oder eines sonstiges „Gönners“ kann sehr schnell dazu führen, dass die Behörde vor Ihrer Tür steht und bei festgestellten Verstößen handeln muss. Auch sollte einem sehr bewusst sein, dass das neue Datenschutzrecht und die sehr intensive Diskussion hierüber absehbar auch Abmahnvereine und andere Geschäftemacher hochmotiviert nach Fehlern bei Ihnen suchen lässt.

Gehen Sie also mit fremden Daten so um, wie Sie es sich selbst beim Umgang mit Ihren persönlichen Daten wünschen!

Kapitel 13: Umgang mit Fotos auf Webseiten

Problemfall Mitarbeiterprofile und -fotos auf der Firmen-Webseite

Für die Verarbeitung von Mitarbeiterdaten gelten in Deutschland Sonderregelungen. § 26 Abs. 1 Satz eins BDSG (neu) regelt, dass Mitarbeiterdaten für die Begründung und Durchführung von Beschäftigungsverhältnissen erhoben, verarbeitet und gespeichert werden dürfen. Hierfür bedarf es aufgrund der gesetzlichen Ausnahme grundsätzlich keiner zusätzlichen Erlaubnis.

In vielen Fällen werden die Daten der Mitarbeiter aber auch über dieses Maß hinaus verwendet. **In vielen Fällen enthält die Homepage der Unternehmen auch Mitarbeiterprofile, um so für den Kunden ein leichtes Auffinden des konkreten Ansprechpartners zu ermöglichen**. Diese Fälle der Veröffentlichung bedürfen in aller Regel der ausdrücklichen Einwilligung des Mitarbeiters. Bei sogenannten „Funktionsträgern", die als offizielle Ansprechpartner fungieren, ist die Veröffentlichung der Basiskommunikationsdaten ohne Einwilligung zulässig. Da es in diesem Bereich allerdings häufig zu Abgrenzungsschwierigkeiten kommt, empfiehlt es sich, stets eine Einwilligung einzuholen. Sollen zusätzlich auch **Fotos der Mitarbeiter** auf der Homepage veröffentlicht werden, bedarf es hierfür ohnehin **zwingend einer Einwilligung.**

Nützliches, Links etc.

Die Bundesbeauftragte für Datenschutz und Informationsfreiheit (hilfreiche Kurzpapiere):
https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/DSGVO_Kurzpapiere.html

Bayerisches Landesamt für Datenschutzaufsicht (Kurzpapiere und Muster):
https://www.lda.bayern.de/de/datenschutz_eu.html

Gesellschaft für Datenschutz und Datensicherheit (mit Praxishilfen):
https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo

Datenschutzerklärungsgenerator der Deutschen Gesellschaft für Datenschutz:
https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/

Übersichtliche Darstellung der gesetzlichen Grundlagen DSGVO, BDSG (neu) sowie weiterer Hintergründe:
https://dsgvo-gesetz.de/

Bundesamt für Sicherheit in der Informationstechnik (BSI) - typische Irrtümer zur IT-Sicherheit:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Sicherheitsirrtuemer/Sicherheitsirrtuemer.html?cms_pos=1

Bundesamt für Sicherheit in der Informationstechnik (BSI) – Kommunikations-Verschlüsselung:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesselung_node.html

Stand dieses Leifadens: Juni 2018

Anlage 1: Checkliste für die ersten Schritte auf dem Weg zur Einhaltung der DSGVO

Maßnahme erfolgt	ja	nein
Schritt 1: Vorbereitung		
Steht die Geschäftsleitung oder der Vorstand hinter den zu treffenden Maßnahmen zur Einhaltung der Datenschutzgesetzgebung und ist dies nachhaltig kommuniziert?		
Sind die Zuständigkeiten für die anstehenden Aufgaben eindeutig verteilt?		
Sind ausreichend zeitliche und materielle Ressourcen eingeplant?		
Ist, sofern gesetzlich notwendig, ein Datenschutzbeauftragter benannt?		
Ist eine Bestandsaufnahme erfolgt, in der festgehalten wurde, in welchen Abläufen des Unternehmens oder Vereins personenbezogene Daten verarbeitet werden?		
Verfügen Sie über ein Verzeichnis Ihrer Verarbeitungstätigkeiten?		
Schritt 2: Umsetzung		
Wissen Sie, auf welche Rechtsgrundlage Sie bisher und künftig Ihre Verarbeitungen stützen können?		
Arbeiten Sie mit Einwilligungen?		
Falls ja, kennen Sie die Anforderungen für eine wirksame Einwilligung?		
Wissen Sie, dass Art. 8 DSGVO besondere Anforderungen für die Einwilligung von Kindern stellt?		
Haben Sie Auftragsverarbeiter eingeschaltet?		
Falls ja, haben Sie mit allen Auftragsverarbeitern die erforderlichen Verträge abgeschlossen?		
Ist sichergestellt, dass Sie der Informationspflicht, dem Auskunftsrecht, dem Recht auf Berichtigung, dem Recht auf Löschung, dem Recht auf Datenübertragbarkeit und dem Widerspruchsrecht gemäß der DSGVO vollständig und in angemessener Zeit nachkommen können?		
Wissen Sie, was Sie im Fall einer Datenschutzverletzung tun müssen?		
Wissen Sie, was unter Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen zu verstehen ist?		
Haben Sie ausreichende Vorkehrungen zur Datensicherheit getroffen?		
Schritt 3: Wiederkehrende Aufgaben		
Ist sichergestellt, dass Sie regelmäßig Änderungen in betrieblichen Abläufen, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben können, entsprechend dokumentieren?		
Ist sichergestellt, dass Sie Ihre Mitarbeiterinnen und Mitarbeiter in regelmäßigen Abständen bezüglich der Einhaltung des Datenschutzes schulen (lassen)?		

Anlage 1a: „kleine Checkliste" für Taxiunternehmen

Anforderungen der Datenschutz-Grundverordnung (DSGVO) an kleine Unternehmen, Vereine, etc.

(Folgendes Musterbeispiel basiert auf einem entsprechend überarbeitetem Muster für Arztpraxen vom Bayerischen Landesamt für Datenschutzaufsicht)

Hinweis:
Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist ein sog. *Verantwortlicher*. Dieser ist insb. dafür verantwortlich, dass er die Anforderungen der DSGVO einhält. In der folgenden Übersicht werden die *wesentlichen* Anforderungen exemplarisch zusammengestellt – ohne Anspruch auf Vollständigkeit. Zu beachten ist daher, dass nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. In diesem Muster wird deshalb der vereinfachte Regelfall angenommen. Erläuterungen zu den jeweiligen Anforderungen sind auf der Rückseite dieses Papiers zu finden.

Musterbeispiel: Kleiner Taxibetrieb

Kurzbeschreibung des Taxiunternehmens

Das kleine Taxiunternehmen auf dem Land betreibt mit 7 Fahrern (einschließlich Unternehmer und Ehefrau) 3 Fahrzeuge bei eigener Vermittlung. Das Unternehmen betreibt eine kleine Webseite mit Hilfe eines Content Management Systems, auf dem online Fahrten gebucht werden können. Ein externer Dienstleister betreut die Webseite und die Unternehmens-IT. Die Datenverarbeitung der Krankenfahrten erfolgt auf eigenen Computern und einem Server innerhalb des Unternehmens.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohn- und Gehaltsabrechnung der Mitarbeiter
- Verarbeitung von Versichertendaten zur Abrechnung mit den Krankenkassen
- Betrieb der Webseite mit der Online-Terminbuchungsmöglichkeit

Wesentliche DS-GVO-Anforderungen für das Taxiunternehmen

A Datenschutzbeauftragter (DSB)
Muss ein DSB benannt werden?
- ☐ ja
- ☒ nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

B Verzeichnis von Verarbeitungstätigkeiten
Ist ein solches Verzeichnis erforderlich?
- ☒ ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)
- ☐ nein

C Datenschutz-Verpflichtung von Beschäftigten
Ist eine solche Verpflichtung durchzuführen?
- ☒ ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)
- ☐ nein

D Information- und Auskunftspflichten
Bestehen irgendwelche Informationspflichten?
- ☒ ja (insb. durch Einwilligungserklärung zur Krankenfahrtenabrechnung sowie auf der Webseite in der Datenschutzerklärung)
- ☐ nein

E Löschen von Daten
Gibt es eine Anforderung zur Datenlöschung?
- ☒ ja (aber erst nach Ablauf gesetzlicher Aufbewahrungs-pflichten)
- ☐ nein

F Sicherheit
Müssen die Daten besonders gesichert werden?
- ☒ ja (da sensible Daten verarbeitet werden, sind weitere Schutzmaßnahmen erforderlich)
- ☐ nein

G Auftragsverarbeitung
Ist ein Vertrag zur Auftragsverarbeitung notwendig?
- ☒ ja (mit dem IT-Betreuer, der die Webseite und die Vermittlungs-IT betreut)
- ☐ nein

H Datenschutzverletzungen
Müssen bestimmte Vorfälle gemeldet werden?
- ☒ ja (aber nur bei relevanten Risiken – eine Einfache Online- Meldung beim Landesdatenschutz ist möglich)
- ☐ nein

I Datenschutz-Folgeabschätzung (DSFA)
Muss eine DSFA im Unternehmen durchgeführt werden?
- ☐ ja
- ☒ nein (da auch bei Gesundheitsdaten nicht immer ein hohes Risiko bei der Datenverarbeitung besteht)

J Videoüberwachung (VÜ)
Besteht eine Ausschilderungspflicht bezüglich VÜ?
- ☐ ja (beim Einsatz von Überfallschutzkameras)
- ☒ nein (da keine Videoüberwachung durchgeführt wird)

Erläuterungen zu den einzelnen Anforderungen:

A Datenschutzbeauftragter (DSB)

In dem Taxiunternehmen findet in aller Regel keine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten statt, die zu einer Benennungspflicht führt. Es ist daher ein DSB nur zu benennen, wenn *mindestens 10 Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind

- DSK-Kurzpapier Nr. 12: *www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf*

B Verzeichnis von Verarbeitungstätigkeiten

Krankenfahrten durchführende Taxi- und Mietwagenunternehmen gehen mit gesundheitsbezogenen Daten um und müssen ein Verzeichnis ihrer Verarbeitungstätigkeiten führen.

- DSK-Kurzpapier Nr. 1: *www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf*
- DSK-Muster-Verzeichnis allgemein: *www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf*

C Datenschutz-Verpflichtung von Beschäftigten

Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt.

- BayLDA Info-Blatt zur Verpflichtung: *www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf*

D Informations- und Auskunftspflichten

Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Zumindest muss er darauf hinweisen, wo die Informationen leicht zugänglich sind (z. B. Flyer, Aushang, Homepage). Die betroffenen Personen haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten.

- DSK-Kurzpapier Nr. 6: *www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf*
- DSK-Kurzpapier Nr. 10: *www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf*

E Löschen von Daten

Sobald keine gesetzliche Grundlage mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. Dies ist in der Regel bspw. der Fall, wenn nach Abschluss des Fahrauftrages 10 Jahre vergangen sind.

- DSK-Kurzpapier Nr. 11: *www.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf*

F Sicherheit

Um sensible Daten wie z.B. Versichertendaten bei Krankenfahrten bei der Verarbeitung zu schützen, sind neben Standardmaßnahmen weitere Maßnahmen zu treffen. Als Standardmaßnahmen zählen u.a. aktuelle Betriebssysteme, Passwortschutz, regelmäßige Backups und Virenscanner. Daneben sollte der Zugriff auf Versichertendaten nur denjenigen in einem Zugriffs- und Berechtigungskonzept gewährt werden, die diese für ihre Arbeit benötigen. Ein Onlinebuchungsformular muss Ende-zu-Ende transportverschlüsselt werden, weshalb die firmeneigene Webseite über eine SSL-Verschlüsselung verfügen sollte.

- BayLDA-Kurzpapier Nr. 1: *www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf*

G Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen (z. B. IT-Wartung) in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich.

- DSK-Kurzpapier Nr. 13: *www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf*
- BayLDA-Formulierungshilfe zum Vertrag: *www.lda.bayern.de/media/muster_adv.pdf*

H Datenschutzverletzungen

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung einer Krankentransportabrechnung oder Verlust auf dem Postweg), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber in Kenntnis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.

- BayLDA-Kurzpapier Nr. 8: *www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf*
- BayLDA-Online-Service zur Meldung: *www.lda.bayern.de/de/datenpanne.html*

I Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

- DSK-Kurzpapier Nr. 5: *www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf*

J Videoüberwachung

Führt ein Verantwortlicher eine Videoüberwachung (z.B. durch Überfallschutzkameras in den Fahrzeugen) durch, ist eine entsprechende Hinweisbeschilderung erforderlich.

- DSK-Kurzpapier Nr. 15: *www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf*

Verzeichnis von Verarbeitungstätigkeiten gem. Artikel 30 Abs. 1 DSGVO	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DSGVO benannt

Anrede Titel

Name, Vorname

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Verarbeitungstätigkeit: Benennung:	**lfd. Nr.:**
Datum der Einführung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)	
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)	
Optional: Name des eingesetzten Verfahrens	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ ☐ ☐
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ ☐ ☐ Besondere Kategorien personenbezogener Daten (Art. 9) ☐

Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offengelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ intern (Zugriffsberechtigte) Abteilung/ Funktion
	☐ extern Empfängerkategorie
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine inter-nationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g) *Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8*

Verantwortlicher Datum Unterschrift

....

Muster: Taxiunternehmen – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:

Max Mustermann
Landstr. 3b
87123 Irgendwohausen

Tel. 0981/123456-0
E-Mail: bestellung@taxi-mustermann.de
Web: www.taxi-mustermann.de

Verarbeitungs-tätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbezogenen Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/ organisatorische Maßnahmen
Lohn-abrechnung	Max Mustermann 0981/123456-1 max@taxi-mustermann.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name, Geburtsdatum • Adresse • Bankverbindungsdaten • Lohn-/Entgeltdaten • ggf. Religionszugehörigkeit • Sozialversicherungsdaten • Steuerdaten (Steuerklasse, Freibeträge) • Berufsgenossenschaftsangaben	Finanzamt	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Verarbeitung von Kundendaten bei der Disposition	Max Mustermann 0981/123456-1 max@taxi-mustermann.de	02.03.2018	Disposition	Fahrgäste	• Name, Adressen • Ggfls. Gesundheitsdaten • Behandlungstermine	Fahrpersonal, ggf. Behandler (Arztpraxen, Med. Zentren)	Keine	10 Jahre (gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Verarbeitung von Versicherten-daten bei der Abrechnung von Krankenfahrten	Gisela Mustermann Meier 0981/123456-0 gisela@taxi-mustermann.de	28.02.2018	Abrechnung	Fahrgäste bei Krankenfahrten	• Behandlungsdaten • (Sozial-)Versicherungsdaten	Krankenkassen beauftragte Abrechnungs-stellen	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Betrieb der Webseite mit Möglichkeit der Onlinebuchung	Justin Nerdie 0981/123456-2 justin@xy-edv.de	02.03.2018	• Betrieb einer Webseite • Onlinebuchung	Fahrgäste Webseiten-besucher	• IP-Adresse • Name und Kontakt • Abholzeit • Abhol- und Zieladresse	Fahrpersonal	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheits-konzept: https, bei Buchung Inhaltsver-schlüsselung
...	...	...	...	...	...	...	...	...	...

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

1 Automatische Updates im Betriebssystem aktivieren
1 Standard-Gruppenverwaltung (z. B. in Windows)
1 Automatische Updates des Browsers aktivieren
1 Aktueller Virenscanner/Sicherheitssoftware
1 Zugriffs- und Berechtigungskonzept
1 Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
1 Papieraktenvernichtung mit Spezial-Shredder
1 Ende-zu-Ende- und Transportverschlüsselung bei Onlinebuchung

Anlage 3: Mustertext und Beispiel für eine Einwilligungserklärung zur Datenverarbeitung bei Krankenfahrten

Mustertext:

Der Unterzeichner erklärt sich damit einverstanden, dass das von ihm beauftragte Beförderungsunternehmen im Rahmen der beauftragten Beförderung personenbezogene Daten des Unterzeichners, insb. Gesundheitsdaten, erfasst, verarbeitet und an Dritte, insb. Krankenkassen und Abrechnungsdienste, bestimmungsgemäß weiterleitet.

Musterbeispiel:

Bestätigung für einen Krankentransport/Materialtransport (Rechnungsfahrt)

Vollständiger Name des Versicherten (bei ges. Bevollmächtigten zusätzlich deren Name)

Versichertennummer | Kostenträger

Der Unterzeichner erklärt sich damit einverstanden, dass das von ihm beauftragte Beförderungsunternehmen im Rahmen der beauftragten Beförderung personenbezogene Daten des Unterzeichners, insb. G[illegible] MUSTERTEXT [illegible] übernommen werden, geht die Rechnung über den nicht ausgeglichenen Betrag zu meinen Lasten und ist mit einer Frist von acht Tagen nach Rechnungsstellung zu begleichen. Eventuelle eigene Ansprüche gegen meinen Kostenträger bleiben hiervon unberührt.

Zuzahlung in Höhe von € wurde geleistet. | Fahrdatum:

Ort und Datum, Unterschrift des Versicherten | Beförderungsbetrieb:

Diese Erklärung gegenüber dem neben genannten Beförderungsbetrieb gilt auch für alle zukünftig verordneten Krankenfahrten mit diesem Betrieb. Ein Widerspruch kann jederzeit und sollte möglichst schriftlich erfolgen.

Anmerkung: Die abgebildete Bestätigung ist ein Muster für Bestätigungen, die bei der Spitzlei GmbH bestellt werden können.

Kontakt:
Spitzlei GmbH
Händelstraße 10
50171 Kerpen
Telefon: +49 2237 922 644
Telefax: +49 2237 922 645

www.spitzlei-abrechnungen.de

Verpflichtung auf das Datengeheimnis

Der Mitarbeiter bestätigt, dass er – sofern er im Rahmen seiner Tätigkeit mit personenbezogenen Daten in Kontakt kommt – umfassend über den Inhalt der wesentlichen gesetzlichen Vorschriften der geltenden Datenschutzbestimmungen (Datenschutz-Grundverordnung - DS-GVO sowie Bundesdatenschutzgesetz – BDSG neu) informiert wurde. Auf Wunsch werden dem Mitarbeiter die wesentlichen Vorschriften auszugsweise zur Verfügung gestellt.

An dieser Stelle wird ergänzend auf die entsprechenden Muster des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie der jeweiligen Datenschutzbehörden der Bundesländer verwiesen, die in der jeweils aktuellen Fassung aus dem Internet (z.B. www.bfdi.bund.de; www.tlfdi.de; www.datenschutz.rlp.de) beziehbar sind.

Dem Mitarbeiter ist in diesem Zusammenhang bekannt, dass er personenbezogene Daten, die ihm im Zusammenhang mit dem Arbeitsverhältnis bekannt geworden sind oder noch bekannt werden, nicht ohne Befugnis verarbeiten (das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten) oder diese Daten Dritten unbefugt mitteilen oder zugänglich machen darf.

Diese Verpflichtung auf das sogenannte „Datengeheimnis“ des Mitarbeiters besteht ohne zeitliche Begrenzung und gilt auch nach Beendigung des Arbeitsverhältnisses fort.

Der Mitarbeiter wird darauf hingewiesen, dass nach § 42 BDSG neu und anderen Strafvorschriften, sowie Bußgeldtatbeständen in der DS-GVO und dem BDSG neu Verstöße gegen Datenschutzbestimmungen durch Freiheits- oder Geldstrafen sowie Bußgelder in zum Teil empfindlicher Höhe geahndet werden können. Der Mitarbeiter wird ferner darauf hingewiesen, dass solche Verstöße eine Verletzung arbeitsvertraglicher Pflichten darstellen und entsprechende arbeitsrechtliche Sanktionen nach sich ziehen können.

Über die Verpflichtung auf das Datengeheimnis und die hieraus für den Mitarbeiter resultierenden Pflichten im Rahmen seines inner- und außerdienstlichen Verhaltens ist er vollständig unterrichtet worden.

_____, den _____ _____

(Unterschrift des Mitarbeiters)

Anlage 5: Vorlage zur Bestellung eines betrieblichen Datenschutzbeauftragten

Bestellung eines betrieblichen Datenschutzbeauftragten

Herrn/Frau

Muster

Mustergasse 1

12345 Musterstadt

Sehr geehrte/r Frau/Herr _____,

ich/wir benennen Sie mit sofortiger Wirkung zur/m Datenschutzbeauftragten gemäß Artikel 37 Abs. 1 b) und c) EU-Datenschutzgrundverordnung (DSGVO) in Verbindung mit § 38 Bundesdatenschutzgesetz (BDSG). In Ihrer Funktion als Datenschutzbeauftragte/r sind Sie der Geschäftsleitung unmittelbar unterstellt.

Zuständiges Mitglied der Geschäftsleitung ist _____

Ihre Aufgaben als Datenschutzbeauftragte/r ergeben sich aus den Artikeln 37 bis 39 DSGVO sowie § 38 BDSG. In der Anwendung Ihrer Fachkunde auf dem Gebiet des Datenschutzes sind Sie weisungsfrei. Bei der Erfüllung Ihrer Aufgaben sind Sie an die Wahrung der Geheimhaltung und der Vertraulichkeit gebunden. Über Ihre Tätigkeit werden Sie der Geschäftsleitung laufend Bericht erstatten.

Erforderliche Organisationsanweisungen schlagen Sie der Geschäftsleitung vor.

_____ _____

Ort, Datum Unterschrift Geschäftsleitung

Mit der Benennung bin ich einverstanden

_____

Unterschrift Datenschutzbeauftragte/r