

DSGVO

WAS HAT SICH VERÄNDERT?

HAT SICH WAS VERÄNDERT?

LEGAL BASICS

REAL LIFE PROBLEMS

Q&A

WORUM GEHT'S EIGENTLICH?

Volkszählungsurteil (BVerfG 1983):
 Recht auf informationelle
 Selbstbestimmung als Teil des
 Persönlichkeitsrechts.

VOLKSZÄHLUNG 1987
Personenbogen

Bitte so markieren

2 34 131 505 5

Rechtsgrundlage:
 Siehe Haushaltsmantelbogen oder Erläuterungsblatt,
 die Bestandteile der Erhebungsvordrucke sind.
 Stichtag: 25. Mai 1987

Bitte Gemeinde angeben:

1 Geburtsangaben

a) Geburtsjahr

b) Geburtsmonat 1. Januar bis 24. Mai
 25. Mai bis 31. Dez.

2 Geschlecht

männlich
 weiblich

3 Familienstand

ledig
 verheiratet
 verwitwet
 geschieden

4 Rechtliche Zugehörigkeit zu einer Religionsgesellschaft *

Römisch-katholische Kirche
 Evangelische Kirche
 Evangelische Freikirche
 Jüdische Religionsgesellschaft
 Islamische Religionsgemeinschaft
 andere Religionsgesellschaften
 keiner Religionsgesellschaft rechtlich zugehörig

5 Welche Staatsangehörigkeit haben Sie? *

deutsch
 griechisch
 italienisch
 übrige EG-Staaten
 jugoslawisch
 türkisch
 sonstige/keine

6 Wird von Ihnen noch eine weitere Wohnung (Unterkunft/Zimmer) in der Bundesrepublik Deutschland einschließlich Berlin (West) bewohnt? *

nein
 ja

Falls ja:

a) Für Verheiratete, die nicht dauernd getrennt leben:
 Ist die hiesige Wohnung die vorwiegend benutzte Wohnung der Familie? nein ja

b) Für alle übrigen Personen:
 Ist die hiesige Wohnung die vorwiegend benutzte Wohnung? nein ja

c) Außerdem für Erwerbstätige, Schüler/Studenten:
 Gehen Sie vorwiegend von der hiesigen Wohnung aus zur Arbeit oder Schule/Hochschule? nein ja

7 Sind Sie erwerbstätig? *

Vollzeit (über 36 Std. in der Woche)
 Teilzeit (bis zu 36 Std. in der Woche)

arbeitslos, arbeitssuchend
 nicht erwerbstätig

Mehrere Antworten möglich

1) Auch Landwirte, mithelfende Familienangeh., Auszubildende, Soldaten, Zivildienstleistende Hausfrau, Hausmann
 2) Maßgebend ist die normalerweise in der Woche geleistete Arbeitszeit Schüler(in), Student(in)

8 Leben Sie überwiegend von? *

Erwerbs-, Berufstätigkeit
 Arbeitslosengeld, -hilfe
 Rente, Pension
 eigenem Vermögen, Vermietung, Verpachtung, Altenteil
 Zuwendungen, Unterhalt durch Eltern, Ehegatten usw.
 sonstigen Unterstützungen (z. B. Sozialhilfe, BAföG)

FÜR ALLE PERSONEN

9 Welchen höchsten allgemeinen Schulabschluß haben Sie? *

Volksschule, Hauptschule
 Realschule/gleichwertiger Abschluß (z. B. Mittlere Reife)
 Hochschulreife (Abitur), Fachhochschulreife

10 a) Welchen höchsten Abschluß an einer berufsbildenden Schule oder Hochschule haben Sie? *

Berufsfachschule (ohne Berufsschule)
 Fachschule
 Fachhochschule (Ing.-Schule, höhere Fachschule)
 Hochschule (einschließlich Lehrerausbildung)

b) Welche Hauptfachrichtung hat dieser Abschluß?

11 Falls Sie eine praktische Berufsausbildung (z. B. Lehre) abgeschlossen haben: *

a) Auf welchen Lehrberuf bezog sich diese Ausbildung?

b) Wie lange dauerte diese Ausbildung? Jahr(e):

12 Bitte Name und Anschrift Ihrer Arbeitsstätte oder Schule/Hochschule angeben. *

Name:
 Straße/Hausnummer:
 PLZ Gemeinde:

13 Welches Verkehrsmittel benutzen Sie hauptsächlich (längste Strecke) auf dem Hinweg zur Arbeit oder Schule/Hochschule? *

kein Verkehrsmittel (zu Fuß)
 Fahrrad
 Pkw
 U-Bahn, S-Bahn, Straßenbahn
 Eisenbahn
 Bus, sonst. öffentl. Verkehrsmittel
 sonstiges (Motorrad, Moped, Mofa)

14 Wieviel Zeit benötigen Sie normalerweise für den Hinweg zur Arbeit oder Schule/Hochschule? *

entfällt, da auf gleichem Grundstück
 unter 15 Minuten
 15 bis unter 30 Minuten
 30 bis unter 45 Minuten
 45 bis unter 60 Minuten
 60 Minuten und mehr

15 Sind Sie zur Zeit tätig als? *

Facharbeiter(in)
 sonstige(r) Arbeiter(in)
 Angestellte(r)
 Auszubildende(r)
 Beamter/Beamtin, Richter(in), Soldat, Zivildienstl. (auch Beamtenanw.)
 Selbständige(r) mit bezahlten Beschäftigten
 ohne bezahlte Beschäftigte
 mithelfende(r) Familienangehörige(r)

16 Zu welchem Wirtschaftszweig (Branche, Behörde) gehört der Betrieb (Firma, Dienststelle), in dem Sie tätig sind? *

17 Welche Tätigkeit, welchen Beruf üben Sie aus? *

18 Falls Sie eine Nebenberufstätigkeit ausüben, handelt es sich um eine

landwirtschaftliche
 nichtlandwirtschaftliche

FÜR ERWERBSTÄTIGE UND SCHÜLER/STUDENTEN

FÜR ERWERBSTÄTIGE

NUR VOM STATISTISCHEN LANDESAMT AUSZUFÜLLEN

Geburtsjahr (1 a)
 2., 3. u. 4. Stelle

Hauptfachrichtung (10 b)

Erlernter Beruf (11 a)

Dauer (11 b)

Arbeitsstätte, Schule/Hochschule (Pendler)
 Land (12) Gemeinde (12) Straße (12)

Hausnummer (12)

Wirtschaftszweig (16)

Ausgeübte Tätigkeit (17)



WORUM GEHT'S EIGENTLICH?

PERSONENBEZOGENE DATEN

- direkt oder indirekt identifizierbar
- besondere Kategorien personenbezogener Daten
rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische/biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung



WORUM GEHT'S EIGENTLICH?

- **AUTOMATISIERTE VERARBEITUNG**
- **SPEICHERUNG IN EINEM DATEISYSTEM**

Art. 2 Abs. 1 DSGVO:

Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.



Datenschutz-Grundverordnung

ACHTUNG!

In unserer Fleischerei fragen wir Sie manchmal nach Ihrem Namen und merken uns, welches Fleisch Ihnen am liebsten ist. Wenn Ihnen das nicht recht ist, rufen Sie beim Betreten der Fleischerei laut:

ICH BIN NICHT EINVERSTANDEN!!

Wir werden dann zukünftig so tun, als würden wir Sie nicht kennen.

GRUNDPRINZIPIEN

1. RECHTMÄSSIGKEIT

2. ZWECKBINDUNG

3. DATENMINIMIERUNG

4. SPEICHERBEGRENZUNG

5. TRANSPARENZ

6. VERTRAULICHKEIT

7. RECHENSCHAFTSPFLICHT

RECHTMÄSSIGKEIT

Was nicht erlaubt ist,
ist verboten.

RECHTMÄSSIGKEIT

... Einwilligung

RECHTMÄSSIGKEIT

EINWILLIGUNG

Freiwillig

Kopplungsverbot

Informiert

Eindeutige, bestätigende Handlung

Klare und einfache Sprache

Hinweis auf Widerrufsrecht

RECHTMÄSSIGKEIT

EINWILLIGUNG



Ja, ich bin damit einverstanden, dass die XXX GmbH mir einmal wöchentlich Informationen zu folgendem Produktsortiment per E-Mail zusendet: Spielwaren, Elektronikgeräte, Bücher. Diese Einwilligung kann Ich jederzeit gegenüber der XXX GmbH widerrufen. Weitere Informationen finden sich in den Datenschutzinformationen.



RECHTMÄSSIGKEIT

... Einwilligung

... Vertragserfüllung

EXKURS: AUFTRAGSVERARBEITUNG

- Websitehosting
- IT-Support
- Lettershop
- Lohnbuchhaltung
- Ableседienste

ABER NICHT:

- Logistik, Spedition
- Handwerker
- Bank

Vereinbarung Auftragsverarbeitung

zwischen der

XXX
XXX
XXX

(nachfolgend „Auftraggeber“)

und

XXX
XXX
XXX

(nachfolgend „Auftragnehmer“)

1. Allgemeines

Die Parteien haben einen Vertrag geschlossen, der die Verarbeitung von personenbezogenen Daten im Auftrag durch den Auftragnehmer beinhaltet („Hauptvertrag“). Diese Vereinbarung Auftragsverarbeitung („AVV“) konkretisiert die Verpflichtungen der Parteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer personenbezogene Daten des Auftraggebers als Auftragsverarbeiter oder personenbezogene Daten Dritter als Unterauftragsverarbeiter des Auftraggebers verarbeitet (nachfolgend insgesamt „Daten“).

2. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Hauptvertrag und ergänzend aus **Anlage 1** dieser AVV ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Die Laufzeit dieser AVV richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser AVV nicht darüberhinausgehende Verpflichtungen ergeben.

3. Rechte und Pflichten des Auftraggebers

Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag

RECHTMÄSSIGKEIT

... Einwilligung

... Vertragserfüllung

... Erfüllung rechtlicher Verpflichtung

RECHTMÄSSIGKEIT

... Einwilligung

... Vertragserfüllung

... Erfüllung rechtlicher Verpflichtung

... Berechtigtes Interesse

RECHTMÄSSIGKEIT

BERECHTIGTES INTERESSE

Art. 6 (1) lit. f) DSGVO

Die Verarbeitung ist nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen der betroffenen Person überwiegen.

- Transparenz
- Widerspruch
- Sensible Daten
- Pseudonymisierung

RECHTMÄSSIGKEIT

BERECHTIGTES INTERESSE



GRUNDPRINZIPIEN

1. RECHTMÄSSIGKEIT

2. ZWECKBINDUNG

3. DATENMINIMIERUNG

4. SPEICHERBEGRENZUNG

5. TRANSPARENZ

6. VERTRAULICHKEIT

7. RECHENSCHAFTSPFLICHT

GRUNDPRINZIPIEN

1. RECHTMÄSSIGKEIT

2. ZWECKBINDUNG

3. DATENMINIMIERUNG

4. SPEICHERBEGRENZUNG

5. TRANSPARENZ

6. VERTRAULICHKEIT

7. RECHENSCHAFTSPFLICHT

GRUNDPRINZIPIEN

1. RECHTMÄSSIGKEIT

2. ZWECKBINDUNG

3. DATENMINIMIERUNG

4. SPEICHERBEGRENZUNG

5. TRANSPARENZ

6. VERTRAULICHKEIT

7. RECHENSCHAFTSPFLICHT

GRUNDPRINZIPIEN

1. RECHTMÄSSIGKEIT

2. ZWECKBINDUNG

3. DATENMINIMIERUNG

4. SPEICHERBEGRENZUNG

5. TRANSPARENZ

6. VERTRAULICHKEIT

7. RECHENSCHAFTSPFLICHT

TRANSPARENZ

INFORMATIONSPFLICHTEN

Verantwortliche Stelle

Verständliche, klare, einfache Sprache

Zwecke und Rechtsgrundlage

Empfänger der Daten

Transfers ins außereuropäische Ausland

Speicherdauer bzw. Löschfristen

Kontaktdaten des Datenschutzbeauftragten

Datenschutzerklärung

Stand: 25. Mai 2018

1. Gegenstand und Geltungsbereich

Wir nehmen den Schutz Ihrer persönlichen Daten sehr ernst. Mit diesen Datenschutzinformationen informieren wir Sie darüber, welche personenbezogenen Daten wir erheben und wie und zu welchen Zwecken diese verarbeitet werden. Wir behandeln Ihre personenbezogenen Daten stets entsprechend der gesetzlichen Datenschutzvorschriften sowie dieser Datenschutzerklärung.

2. Verantwortliche Stelle

XYZ GmbH
Datenschutzallee 1
12345 Berlin
T: +49 (0)30 1234567
F: +49 (0)30 1234568
E: info@xyz.de

3. Datenschutzbeauftragter

Christian Schmoll
Rechtsanwalt, Fachanwalt IT-Recht
Kaiserplatz 2
80803 München
schmoll@dp.institute|

Jeder Betroffene kann sich jederzeit bei allen Fragen und Anregungen zum Datenschutz direkt an unseren Datenschutzbeauftragten wenden.

4. Besuch der Website

Bei jedem Aufruf unserer Website erfasst unser System automatisiert Daten und Informationen vom Computernetzwerk des aufrufenden Rechners. Damit die Seiten in Ihrem Browser dargestellt werden können

Videoüberwachung



die Videoüberwachung:

Frau Maria Schultes

Datenschutzbeauftragten:

@musterfirma.de

Grundlage:

GVO

Personen, die verfolgt werden:

Zweck: Schutz des Eigentums

weitere Informationen finden Sie unter:

[/datenschutz](#)



TRANSPARENZ

INFORMATIONSPFLICHTEN

*Pflichtfelder

Ihre Angaben werden nur zum Zwecke der Verarbeitung dieser Kontaktanfrage genutzt und gespeichert, sowie nicht ohne Ihr Einverständnis an Dritte weitergegeben. Sie haben jederzeit das Recht auf Auskunft, Änderung oder Löschung Ihrer persönlichen Daten.

Ausführliche Informationen finden Sie in unserer [Datenschutzerklärung](#).

- Ja, ich stimme der Verarbeitung meiner persönlichen Daten zu.
- Ja, ich habe die Bestimmungen zum Datenschutz gelesen und bin mit ihnen einverstanden.

Anfrage versenden

Erklärung

ndert.

ben.



TRANSPARENZ

BETROFFENENRECHTE

Auskunft

Berichtigung

Löschung/Sperrung

Übertragbarkeit

GRUNDPRINZIPIEN

1. RECHTMÄSSIGKEIT

2. ZWECKBINDUNG

3. DATENMINIMIERUNG

4. SPEICHERBEGRENZUNG

5. TRANSPARENZ

6. VERTRAULICHKEIT

7. RECHENSCHAFTSPFLICHT

VERTRAULICHKEIT & INTEGRITÄT

Art. 32 Abs. 1 DSGVO:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.**

VERTRAULICHKEIT & INTEGRITÄT

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Bei der XYZ GmbH sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit [§ 4, Art. 32 DSGVO](#) getroffen worden:

1. VERTRAULICHKEIT

1.1 Zutrittskontrolle

Die Büroräume der XYZ GmbH befinden sich in einem Bürohaus in Musterstadt. Die Zugänge zum Bürohaus und auch zu den Büroräumen der XYZ GmbH sind Tag und Nacht verschlossen. Zugang zu dem Bürohaus haben nur der Vermieter und die Mieter der Büroräume. Es kommt ein elektronisches Schließsystem zum Einsatz, das vom Vermieter verwaltet wird. Jeder Mieter des Bürohauses hat jedoch die Möglichkeit, die jeweils ausgehändigten Transponder-Schlüssel selbst zu verwalten und elektronische Zutrittsrechte zu erteilen und zu entziehen. Dies wird von der Personalabteilung der XYZ GmbH verwaltet.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu dem Bürohaus und dann den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.

Jeder Besucher wird in einem Besucherbuch protokolliert und dann von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet.

Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Die Eingänge und Fenster des Bürohauses und auch der Büroräume der XYZ GmbH sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Unabhängig davon wird die Alarmanlage täglich jedoch stets um 21 Uhr automatisch aktiviert.

1.2 Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von XYZ GmbH getroffen worden:

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag kann auch über die Personalabteilung gestellt werden.

Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme der XYZ GmbH erfolgen stets über verschlüsselte Verbindungen.

Auf den Servern der XYZ GmbH ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist. [§ 1](#)

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden. [§ 1](#)

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt. [§ 1](#)

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. [§ 1](#)

Passwörter werden grundsätzlich verschlüsselt gespeichert. [§ 1](#)

1.3→ Zugriffskontrolle [§ 1](#)

Berechtigungen für IT-Systeme und Applikationen der XYZ GmbH werden ausschließlich von Administratoren eingerichtet. [§ 1](#)

Berechtigungen werden grundsätzlich nach dem Need-to-know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind. [§ 1](#)

Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Der Antrag kann auch bei der Personalabteilung gestellt werden. [§ 1](#)

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten. [§ 1](#)

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet. [§ 1](#)

Alle Mitarbeiter bei XYZ GmbH sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen. [§ 1](#)

Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren. [§ 1](#)

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert. [§ 1](#)

1.4→ Trennung [§ 1](#)

Alle von XYZ GmbH für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet. [§ 1](#)

1.5→ Pseudonymisierung & Verschlüsselung [§ 1](#)

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen. [§ 1](#)

Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz. [§ 1](#)

2.→ INTEGRITÄT [§ 1](#)

2.1→ Eingabekontrolle [§ 1](#)

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von XYZ GmbH im Auftrag verarbeitet werden, wird grundsätzlich protokolliert. [§ 1](#)

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. [Benutzeraccounts](#) dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden. [§ 1](#)

2.2→ Weitergabekontrolle [§ 1](#)

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von XYZ GmbH erfolgt, darf jeweils nur in dem Umfang, wie erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist. [§ 1](#)

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert. [§ 1](#)

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen. [§ 1](#)

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei XYZ GmbH im Zusammenhang mit Kundenprojekten untersagt. [§ 1](#)

Mitarbeiter bei XYZ GmbH werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden. [§ 1](#)

3.→ VERFÜGBARKEIT UND BELASTBARKEIT [§ 1](#)

Daten auf Serversystemen von XYZ GmbH werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht. [§ 1](#)

Das Einspielen von Backups wird regelmäßig getestet. [§ 1](#)

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst. [§ 1](#)

Es gibt bei XYZ GmbH einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet. [§ 1](#)

4.→ AUFTRAGSKONTROLLE [§ 1](#)

Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union. [§ 1](#)

Bei der XYZ GmbH ist ein betrieblicher Datenschutzbeauftragter benannt. [§ 1](#)

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführten Audit durch den Datenschutzbeauftragten von XYZ GmbH abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert. [§ 1](#)

5.→ PRIVACY BY DESIGN UND PRIVACY BY DEFAULT [§ 1](#)

Bei der XYZ GmbH wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirmmasken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder deaktiviert werden. [§ 1](#)

Die Software der XYZ GmbH unterstützt sowohl die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden. [§ 1](#)

6.→ VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG [§ 1](#)

Bei der XYZ GmbH ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird. [§ 1](#)

Es ist ein Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt. [§ 1](#)

Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst. [§ 1](#)

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden. [§ 1](#)

Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen. [§ 1](#)



VERTRAULICHKEIT & INTEGRITÄT

Zugriffsrechte

Passwörter

Verschlüsselung (Listen per E-Mail)

USB-Sticks

“Shadow IT”: Private Dropbox, WhatsApp etc.

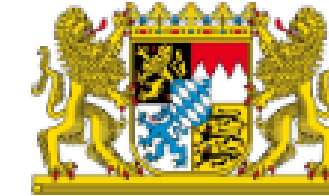
Aktenschranke etc.

Virenschutz & Firewalls

VERTRAULICHKEIT & INTEGRITÄT

MELDEPFLICHT

Bayerisches Landesamt für
Datenschutzaufsicht



BayLDA Online-Services ▾ Datenschutz ▾ Veröffentlichungen ▾ Unsere Behörde ▾

Suche...



[Home](#) > [Online-Services](#) > [Datenschutzverletzung](#)

Meldung einer Datenschutzverletzung für Verantwortliche

Im Falle einer Verletzung des Schutzes personenbezogener Daten können bayerische Verantwortliche aus dem nicht-öffentlichen Bereich (d.h. Unternehmen, Vereine und Verbände, etc.) über diesen Online-Service eine offizielle Mitteilung nach Art. 33 DS-GVO an uns als zuständige Datenschutzaufsichtsbehörde durchführen. Als Meldenachweis erhält der Verantwortliche nach Absenden eine eigene ID, die dem gemeldeten Vorgang zugewiesen wird und als Nachweis der Meldung inklusive Meldezeitpunkt verwendet werden kann.

Wir weisen ausdrücklich darauf hin, dass dieser Online-Service nur Verantwortlichen im Zuständigkeitsbereich des BayLDA zur Verfügung steht. Privatpersonen, die von einem Vorfall selbst betroffen sind, können den hierfür eingerichteten Online-Service "[Datenschutz-Beschwerde](#)" nutzen.

Pflichtfelder sind mit einem * markiert.

Art der Meldung

- Neumeldung
- Folgemeldung

Verantwortliche Organisation

Was ist passiert? *

Bitte wählen Sie eine Kategorie

Wo ist der Vorfall passiert?



GRUNDPRINZIPIEN

1. RECHTMÄSSIGKEIT

2. ZWECKBINDUNG

3. DATENMINIMIERUNG

4. SPEICHERBEGRENZUNG

5. TRANSPARENZ

6. VERTRAULICHKEIT

7. RECHENSCHAFTSPFLICHT

RECHENSCHAFTSPFLICHT

GUILTY

until proven innocent



RECHENSCHAFTSPFLICHT

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T		
Verfahrensanlage (VZ)	Umfeld des VZ	Beschreibung und Zweck des VZ	Qualifizierung der Daten	Kategorie betroffener Personengruppen	Kategorie personenbezogener Daten	Verbreitung des Daten (Art 6)	Rechtsgrundlage des VZ	Informationspflichten	Rechtsvorschriften	Anderer Verarbeitungszweck	Systeme und sonstige Verarbeitung	Speicherort/Weitergabe	Verbreitung/Aufgabenerfüllung	Übermittlung in Drittstaaten	Datenschutz	Art der Verarbeitung	Aggregierte Daten/Verbreitung der Daten und sonstiges	Aufbewahrung und Löschung	Rechenschaft und Dokumentation		
1	Prüfung, Bewertung, Hohe																				
2	Übersetzung	Verkauf von XYZ über den OnlineShop	Übersetzung aller für den jeweiligen Verkaufszweck relevanten Daten über das Shopsystem, Shopsystem bis eine Email an den Kunden/Bestellern (z.B. Bestellvorgang) und eines weiteren E-Mail an die verantwortliche Stelle, die die Bestellung bearbeitet, die verantwortliche Stelle übernimmt die Verantwortlichkeit im ERP-System und sendet eine Auftragsbestätigung.	Kunden, Interessenten	Personaldaten (Name, Adresse), Kontaktdaten (E-Mail, Telefonnummer, Fax, Messenger), Vermögensdaten (Bankdaten, IBAN, Zahlungsinformationen)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		Shopsystem XYZ, E-Mail, ERP-System	Mitarbeiter der verantwortlichen Stelle ("Hand in Hand"), Support-Adressen beim Shopsystem bei XYZ, Support und Werbung Shopsystem durch XYZ (Shop/Ad/Personalisierte Daten möglich)	nein	nein	nein	nein	nein	nein	nein	nein	
3	Bestellvorgang "Standard"	Ingenieurin und Abwicklung von Bestellungen über E-Mail, Fax, Telefon (E-Mail/Telefon)	Bestellvorgang über Verkauf von Software über E-Mail, Fax, Telefon (E-Mail/Telefon)	Kunden, Interessenten	Personaldaten (Name, Adresse), Kontaktdaten (E-Mail, Telefonnummer, Fax, Messenger), Vermögensdaten (Bankdaten, IBAN, Zahlungsinformationen)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		E-Mail, Telefon, Fax, ERP-System	E-Mail-Belegserver, Mitarbeiter der verantwortlichen Stelle	nein	nein	nein	nein	nein	nein	nein	nein	
4	Zahlungsbuchführung	Abwicklung von Zahlungen im Rahmen des Verkauf	Zahlungsgüter werden vom Käufer im Rahmen des Kaufvorgangs eingezogen	Kunden	Personaldaten (Name, Adresse), Kontaktdaten (E-Mail, Telefonnummer, Fax, Messenger), Vermögensdaten (Bankdaten, IBAN, Zahlungsinformationen)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		OnlineShop (bei Online-Bestellung) ERP-System	PayPal, Klarna (Bildererkennung), Company Director für Verlinkung von Kreditkartenzahlungen, Barista/Praxisdienstleister	nein	nein	nein	nein	nein	nein	nein	nein	nein
5	Bestellprüfung	Bestellprüfung der Kunden bei Vorbestellung als Bestellvorgang/Bestellung vom Kunden	Bestellprüfung über bestellungs.com Kunden	Kunden	Bestell, Bestellung	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		ERP-System, Datenübermittlung an Dienstleister/Anbieter	Auswählbar (DVG)	nein	nein	nein	nein	nein	nein	nein	nein	
6																					
7																					
8	Marketing und Vertrieb																				
9	Website	Bereitstellung der Unternehmens-Website	Übersetzung von Daten der User der Website	Websitebenutzer	IP-Adresse des aufrufenden Rechners, Browser/Verhalten des aufrufenden Rechners, Name der aufrufenden Client, Datum und Uhrzeit des Abrufs, Übergang, Dauer, Übergang, User-ID	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		Hosting bei XYZ	Mitarbeiter der verantwortlichen Stelle ("Hand in Hand"), Support-Adressen beim Shopsystem bei XYZ, Werbeplätze, ZXX (Shop/Ad/Personalisierte Daten möglich)	nein	nein	nein	nein	nein	nein	nein	nein	
10	Newsletter	Verkauf von E-Mail-Newslettern	Registrierung von Usern auf der Website, zudem Zustellung an Bestellschritte	Newsletter-Abonnenten, Kunden	E-Mail-Adresse, Name, IP-Adresse, Opt-In-Daten, Interessenten (Klienten/ID)	nein	Mit Bestätigung Art 6 Abs. 1 lit. b DSGVO, Einwilligung im Bestellschritt Art 6 Abs. 1 lit. f DSGVO, 7 Abs. 1 UWG, Newsletter-Datung Art 6 Abs. 1 lit. b DSGVO	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden	Wahlfreiheit der Einwilligung bzw. Widerspruch gegen weitere Verarbeitung möglich, Anmeldebestätigung und Löschung bzw. Sperrung der Daten möglich		E-Mail-Marketing Provider MailChimp	Mitarbeiter der verantwortlichen Stelle ("Hand in Hand"), Support-Adressen beim Shopsystem	nein	nein	nein	nein	nein	nein	nein	nein	
11	Website-Tracking	Speicherung der IP-Adressen der besuchten Webseiten und der Verwendung durch die Tracking Software beim Besuch der Website	Übersetzung des Navigationsverhaltens der Websitebenutzer	Websitebenutzer	IP-Adresse der Websitebenutzer (Anonymisierung von IP-Adressen), Browser/Verhalten des aufrufenden Rechners, Name der aufrufenden Client, Datum und Uhrzeit des Abrufs, Übergang, Dauer, Übergang, User-ID	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Wahlfreiheit der Einwilligung bzw. Widerspruch gegen weitere Verarbeitung möglich, Anmeldebestätigung und Löschung bzw. Sperrung der Daten möglich		Google über Cookies	Google Analytics	nein	nein	nein	nein	nein	nein	nein	nein	
12	Analytics	Verknüpfung von Kunden- und Interessenten mit IP-Adressen	Verknüpfung von Kunden- und Interessenten mit IP-Adressen	Kunden, Interessenten	Name, Firma, Kontaktdaten, Vermögensdaten (ggf)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Wahlfreiheit der Einwilligung bzw. Widerspruch gegen weitere Verarbeitung möglich, Anmeldebestätigung und Löschung bzw. Sperrung der Daten möglich		ERP-System, Shopsystem	nein	nein	nein	nein	nein	nein	nein	nein	nein	
13	Marketing von Kunden- und Interessenten im ERP-System	Speicherung von Kunden- und Interessenten für Marketing-Zwecke und von Zweck der Durchführung von Marketingmaßnahmen	Kunden, Interessenten	Kunden, Interessenten	Personaldaten (Name, Adresse), Kontaktdaten (E-Mail, Telefonnummer, Fax, Messenger), Vermögensdaten (Bankdaten, IBAN, Zahlungsinformationen)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Wahlfreiheit der Einwilligung bzw. Widerspruch gegen weitere Verarbeitung möglich, Anmeldebestätigung und Löschung bzw. Sperrung der Daten möglich		ERP-System	nein	nein	nein	nein	nein	nein	nein	nein	nein	
14																					
15	Personal																				
16	Bestellung/Bestellvorgang	Personalbuchung, Anrechnung von Bestellungen für eine mögliche Bestellung	Bestellvorgang über E-Mail	Besteller	Personaldaten (Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Ausbildung, Berufstätigkeit etc.)	nein	Art 6 Abs. 1 lit. b oder DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		E-Mail-Belegserver, Besteller	nein	nein	nein	nein	nein	nein	nein	nein	nein	
17	Personalbuchung	Personalbuchung zur Verwaltung der Mitarbeiter	Übersetzung im Rahmen der Arbeitsverhältnisse	Mitarbeiter, ehemalige Mitarbeiter	Personaldaten der Mitarbeiter	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		HR-System (Büro/HR), Personal "Personal"	nein	nein	nein	nein	nein	nein	nein	nein	nein	
18																					
19	Marketing																				
20	Engpassüberwindung und Leistungsüberwindung	Verknüpfung und Anrechnung der Kunden, Interessenten der Bestellung von Kaufverträgen unter der Kundennummer, Anrechnung	Bestellvorgang über E-Mail	Mitarbeiter, ehemalige Mitarbeiter	Personaldaten (Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Ausbildung, Berufstätigkeit etc.)	nein	Art 6 Abs. 1 lit. b oder DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		HR-System (Büro/HR), Personal "Personal"	nein	nein	nein	nein	nein	nein	nein	nein	nein	
21	Personalbuchung	Übersetzung der Personalbuchung, Anrechnung	Bestellvorgang über E-Mail	Mitarbeiter, ehemalige Mitarbeiter	Personaldaten (Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Ausbildung, Berufstätigkeit etc.)	nein	Art 6 Abs. 1 lit. b oder DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		HR-System (Büro/HR), Personal "Personal"	nein	nein	nein	nein	nein	nein	nein	nein	nein	
22	Erstellung	Erstellung zur Planung, Bewertung und Kontrolle aller Personalmaßnahmen	Bestellvorgang über E-Mail	Mitarbeiter, ehemalige Mitarbeiter	Personaldaten (Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Ausbildung, Berufstätigkeit etc.)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		HR-System (Büro/HR), Personal "Personal"	nein	nein	nein	nein	nein	nein	nein	nein	nein	
23	Planung und Abrechnung von Dienstleistungen	Abrechnung von Dienstleistungen	Mitarbeiter wählen Sperrverträge ein	Mitarbeiter, ehemalige Mitarbeiter	Personaldaten (Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Ausbildung, Berufstätigkeit etc.)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		HR-System, Burea/DATV	nein	nein	nein	nein	nein	nein	nein	nein	nein	
24																					
25																					
26	IT-Systeme																				
27	Personalbuchung, Wartung, Pflege	Personalbuchung zur Verwaltung von Mitarbeitern, zur Verbesserung der Performance oder anderer Analyse und Anpassungen an Veränderungs, Beratung und Administration der IT-Infrastruktur und der Schulung, auch in Form von	Möglicher Zugriff auf gespeicherte personalbezogene Daten kann nicht ausgeschlossen werden	Kunden, Interessenten, Mitarbeiter, Bewerber, ehemalige Mitarbeiter, Lieferanten, sonstige Auftraggeber (Personen)	Alle personalbezogenen Daten, die in der Software hinterlegt sind	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		ERP-System, Software, Schulung, Cloud	nein	nein	nein	nein	nein	nein	nein	nein	nein	
28	Personalbuchung, Wartung, Pflege	Personalbuchung zur Verwaltung von Mitarbeitern, zur Verbesserung der Performance oder anderer Analyse und Anpassungen an Veränderungs, Beratung und Administration der IT-Infrastruktur und der Schulung, auch in Form von	Möglicher Zugriff auf gespeicherte personalbezogene Daten kann nicht ausgeschlossen werden	Kunden, Interessenten, Mitarbeiter, Bewerber, ehemalige Mitarbeiter, Lieferanten, sonstige Auftraggeber (Personen)	Alle personalbezogenen Daten, die in der Software hinterlegt sind	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		ERP-System, Software, Schulung, Cloud	nein	nein	nein	nein	nein	nein	nein	nein	nein	
29	Audit	Interne Audit der technischen Überwachung von Prozessen zur Erfüllung von gesetzlichen Standards oder Richtlinien im Unternehmen	Möglicher Zugriff auf gespeicherte personalbezogene Daten kann nicht ausgeschlossen werden	Kunden, Interessenten, Mitarbeiter, Bewerber, ehemalige Mitarbeiter, Lieferanten, sonstige Auftraggeber (Personen)	Alle personalbezogenen Daten, die in der Software hinterlegt sind	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		ERP-System, Software, Schulung, Cloud	nein	nein	nein	nein	nein	nein	nein	nein	nein	
30	E-Mail	Bereitstellung, Verwaltung und Anrechnung der E-Mail-Kommunikation, Datenanrechnung, effiziente Prozessgestaltung	E-Mail-Kommunikation	Kunden, Interessenten, Mitarbeiter, Bewerber, ehemalige Mitarbeiter, Lieferanten, sonstige Auftraggeber (Personen)	E-Mail-Adresse, Vermögensdaten, Name, Mitarbeiter	nein	Art 6 Abs. 1 lit. b, a, c DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		Cloud-Exchange-Server	nein	nein	nein	nein	nein	nein	nein	nein	nein	
31	Interessengruppen (einschließlich gewerkschaftlicher Interessen)	Bereitstellung des Interessengruppen	Übersetzung und Verwaltung der Interessen	Mitarbeiter, Bewerber, ehemalige Mitarbeiter, Lieferanten, sonstige Auftraggeber (Personen)	Interessengruppen (Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Ausbildung, Berufstätigkeit etc.)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		LAN/WLAN	nein	nein	nein	nein	nein	nein	nein	nein	nein	
32	Interessengruppen (einschließlich gewerkschaftlicher Interessen)	Bereitstellung und Verwaltung der Interessen	Übersetzung und Verwaltung der Interessen	Mitarbeiter, Bewerber, ehemalige Mitarbeiter, Lieferanten, sonstige Auftraggeber (Personen)	Interessengruppen (Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Ausbildung, Berufstätigkeit etc.)	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		Interne/Cloud	nein	nein	nein	nein	nein	nein	nein	nein	nein	
33	Personalbuchung, Wartung, Pflege	Personalbuchung zur Verwaltung von Mitarbeitern, zur Verbesserung der Performance oder anderer Analyse und Anpassungen an Veränderungs, Beratung und Administration der IT-Infrastruktur und der Schulung, auch in Form von	Möglicher Zugriff auf gespeicherte personalbezogene Daten kann nicht ausgeschlossen werden	Kunden, Interessenten, Mitarbeiter, Bewerber, ehemalige Mitarbeiter, Lieferanten, sonstige Auftraggeber (Personen)	Alle personalbezogenen Daten, die in der Software hinterlegt sind	nein	Art 6 Abs. 1 lit. b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		HR-System (Büro/HR), Personal "Personal"	nein	nein	nein	nein	nein	nein	nein	nein	nein	
34	Offene Anwendung und sonstige Anwendungen	Speicherung und Verarbeitung personenbezogener Daten	Speicherung durch Mitarbeiter	Kunden, Interessenten, Mitarbeiter, Bewerber, ehemalige Mitarbeiter, Lieferanten, sonstige Auftraggeber (Personen)	Alle von den betroffenen Personengruppen erfassten Daten	nein	Art 6 Abs. 1 lit. b, a, b DSGVO	Information in den Daten/Informations auf der Website	Auswählbar, Löslich und sonstige Betroffenen für können, es keine besonderen Aufmerksamkeitspflichten eingetragenen, manuell eingetragene werden		Offen/Cloud	nein	nein	nein	nein	nein	nein	nein	nein	nein	
35																					

SANKTIONEN

1. Bußgelder

2. Untersagungen

3. Abmahnungen

4. Sammelklagen

5. Reputationsschaden

DATENSCHUTZBEAUFTRAGTER

Unterrichtung, Beratung

Überwachung

Ansprechpartner

LEGAL BASICS

REAL LIFE PROBLEMS

Q&A

COOKIES

Ihre Einstellungen zu Cookies für dieses Website

Wählen Sie aus, ob diese Webseite lediglich funktionelle Cookies und/oder Marketing Cookies, wie nachfolgend beschrieben, verwenden darf:

<input checked="" type="checkbox"/> Erforderliche Cookies Diese Cookies lassen die Webseite richtig funktionieren	Erlaubte Funktionen <ul style="list-style-type: none">- Sichert die Stabilität der Webseite- Bietet sicheren Log-In- Speichert, wie weit Sie in einer Bestellung sind- Speichert Ihre Log-In Daten- Speichert Ihren Warenkorb
<input type="checkbox"/> Analytische Cookies Diese Cookies ermöglichen uns eine Analyse der Webseite, damit wir die Performance unserer Seiten messen und verbessern können.	Nicht erlaubte Funktionen <ul style="list-style-type: none">- Ermöglicht uns, das Nutzer Erlebnis zu verbessern- Ermöglicht Ihnen das Teilen von Seiten auf Sozialen Netzwerken- Erlaubt Ihnen, Kommentare zu posten- Liefert Anzeigen, die zu Ihren Interessen passen, auch auf sozialen Medien
<input type="checkbox"/> Social Media Über diese Cookies können Sie sich mit Ihren Social Media Kanälen verbinden und Reviews lesen.	
<input type="checkbox"/> Marketing Cookies Wir nutzen diese Cookies, um Ihnen auf Ihre Interessen zugeschnittene Werbung anzuzeigen, innerhalb und außerhalb der Philips Webseiten.	

Ihre Einstellungen zu Cookies für dieses Website

Wählen Sie aus, ob diese Webseite lediglich funktionelle Cookies und/oder Marketing Cookies, wie nachfolgend beschrieben, verwenden darf:

<input type="checkbox"/> Erforderliche Cookies Diese Cookies lassen die Webseite richtig funktionieren	Erlaubte Funktionen <ul style="list-style-type: none">- Sichert die Stabilität der Webseite- Bietet sicheren Log-In- Speichert, wie weit Sie in einer Bestellung sind- Speichert Ihre Log-In Daten- Speichert Ihren Warenkorb- Ermöglicht uns, das Nutzer Erlebnis zu verbessern- Ermöglicht Ihnen das Teilen von Seiten auf Sozialen Netzwerken- Erlaubt Ihnen, Kommentare zu posten- Liefert Anzeigen, die zu Ihren Interessen passen, auch auf sozialen Medien
<input type="checkbox"/> Analytische Cookies Diese Cookies ermöglichen uns eine Analyse der Webseite, damit wir die Performance unserer Seiten messen und verbessern können.	
<input type="checkbox"/> Social Media Über diese Cookies können Sie sich mit Ihren Social Media Kanälen verbinden und Reviews lesen.	
<input checked="" type="checkbox"/> Marketing Cookies Wir nutzen diese Cookies, um Ihnen auf Ihre Interessen zugeschnittene Werbung anzuzeigen, innerhalb und außerhalb der Philips Webseiten.	



E-MAIL-WERBUNG

BDSG

>>>

DSGVO

TMG

>>>

ePrivacy-VO

UWG

E-MAIL-WERBUNG

§ 7 Gesetz gegen den unlauteren Wettbewerb (UWG)

Postwerbung	<ul style="list-style-type: none">• Grundsätzlich zulässig, solange nicht erkennbar unerwünscht
Telefonwerbung	<ul style="list-style-type: none">• Nur mit Einwilligung<ul style="list-style-type: none">• Verbraucher: nicht ohne vorherige ausdrückliche Einwilligung• B2B: nicht ohne zumindest „mutmaßliche“ Einwilligung
E-Mail- und SMS-Werbung	<ul style="list-style-type: none">• Nur mit Einwilligung• Enge Ausnahme für Werbung gegenüber Bestandskunden<ul style="list-style-type: none">• für ähnliche Waren und Dienstleistungen• unter Beachtung von Informationspflichten über das Widerspruchsrecht: bei Erhebung und in jeder Werbung
Telefaxwerbung	<ul style="list-style-type: none">• Immer nur mit Einwilligung

Anwendung UWG auf Non-Profit



E-MAIL-WERBUNG

Ja, ich bin damit einverstanden, dass die XXX GmbH mir einmal wöchentlich Informationen zu folgendem Produktsortiment per E-Mail zusendet: Spielwaren, Elektronikgeräte, Bücher.
Diese Einwilligung kann Ich jederzeit gegenüber der XXX GmbH widerrufen. Weitere Informationen finden sich in den [Datenschutzinformationen](#).

E-MAIL-WERBUNG



Sehr geehrter Herr Schmoll,

Sie haben momentan 89 neue Event-Benachrichtigungen in Ihrem Posteingang auf XING.

Die neueste Nachricht ist von [REDACTED] und hat den Betreff "Einladung zum Event "Der Geld-Plan: Die 6 Geheimnisse wirklich erfolgreicher Geschäfte" - kostenloses Webinar"

Jetzt auf XING lesen:

<http://www.xing.com/app/message?op=show&box=EVENT&id=522836&dpt=sysm&ttp=mail&plf=own&pid=event-invite&xtr=lnk>

WhatsApp



- 1 Create a new contact for our number [+49 157 92351478](tel:+4915792351478).
- 2 Send "Start" to this contact via WhatsApp.

Contact [+4915792351478](tel:+4915792351478)



Darf ich Teilnehmer an einem Event auch ohne Newsletter-Opt-In zu anderen Events oder z.B. zu Folgeveranstaltungen per E-Mail einladen?

E-Mail-Werbung bei bestehender Kundenbeziehung

- E-Mail-Adresse im Zusammenhang mit dem Verkauf einer Ware/Dienstleistung von dem Kunden erhalten
- verwendet für Direktwerbung für eigene ähnliche Waren/Dienstleistungen
- der Kunde hat der Verwendung nicht widersprochen
- der Kunde wurde bei Erhebung der Adresse klar und deutlich darauf hingewiesen, dass er der Verwendung jederzeit widersprechen kann



E-MAIL-WERBUNG

Darf ich Teilnehmer an einem Event auch ohne Newsletter-Opt-In zu anderen Events oder z.B. zu Folgeveranstaltungen per E-Mail einladen?

Wir schicken Ihnen ihre Teilnahmebestätigung an Ihre angegebene E-Mail-Adresse. Zudem werden wir Ihnen zukünftig Einladungen zu weiteren ähnlichen Events, die für Sie interessant sein könnten, zusenden. Dieser Zusendung können Sie jederzeit durch eine E-Mail an unsubscribe@xyz.de widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen. Zudem ist in jeder E-Mail ein Abmeldelink enthalten. Nach Erhalt ihres Widerspruchs werden wir diese Zusendungen unverzüglich einstellen.



EVENTS

Wie lange darf und muss ich denn die Teilnehmerdaten nach einem Event aufbewahren?

Darf ich Teilnehmerlisten weitergeben?

Sind Schwerbehindertenrabatte datenschutzrechtlich problematisch?



**URHEBERRECHT:
DER FOTOGRAF**

**DATENSCHUTZRECHT:
DAS MOTIV**

Fotografieren & Veröffentlichen = Verarbeitung personenbezogener Daten

§ 23 KUG:

Ohne (...) Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. **Bildnisse** aus dem Bereiche der **Zeitgeschichte**;
2. **Bilder**, auf denen die **Personen nur als Beiwerk** neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. **Bilder von Versammlungen, Aufzügen** und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;

VERÖFFENTLICHUNG: KUG

EINWILLIGUNG

AUSNAHMEN FÜR EVENTS

AUFNAHME: DSGVO

EINWILLIGUNG

BERECHTIGTES INTERESSE



BAYLDA: VERARBEITUNG VON BILDERN IM RAHMEN VON INTERESSENABWÄGUNG IST MÖGLICH, ABER NICHT

- **BEI KINDERN,**
- **VON BILDERN AUS DER PRIVAT- ODER INTIMSPHÄRE (Z.B. PARTY, URLAUB, NACKTBILDER),**
- **BILDERN, DIE AUF BES. KATEGORIEN PERSONENBEZOGENER DATEN HINWEISEN**



Hinweis (z.B. in Einladung und am Eingang):

- **dass Fotos angefertigt werden,**
- **für welchen Zweck Fotos gemacht werden,**
- **ob, und wenn ja, wo Fotos veröffentlicht werden sollen**
- **an wen sich betroffene Person bei Datenschutzfragen wenden kann
(Widerspruch, Löschung u.a.)**



Bundesverband
Deutscher
Stiftungen

Jobs

Stiftungen

Themen

d) Veranstaltungen des Bundesverbands Deutscher Stiftungen

Zu Dokumentationszwecken werden auf Veranstaltungen des Bundesverbands Deutscher Stiftungen wie bspw. dem Deutschen Stiftungstag Fotos und Videos aufgenommen. Der Bundesverband Deutscher Stiftungen verwendet diese im Rahmen seiner Berichterstattung, für seine allgemeine Presse- und Öffentlichkeitsarbeit, insbesondere in den Sozialen Medien, auf der Webseite des Bundesverbands und in sonstigen Verbandsmedien. Ferner kann das Material für die Öffentlichkeitsarbeit des Bundesverbands Deutscher Stiftungen als Presseinformation an andere Medien weitergegeben werden.

Sie haben das Recht, der Anfertigung von Fotos und Videos, die Sie betreffen, sowie deren Verwendung zu widersprechen.



- **Einwilligung im Arbeitsverhältnis?**
- **Konkret, individuell (keine BV), freiwillig**
- **Widerruf?**
- **Einwilligung Minderjähriger?**



SOCIAL MEDIA

05.06.2018 | 15:54 Uhr

“Abschalten der Fanpages derzeit einzig rechtskonforme Lösung”: Was der Anwalt zum EuGH-Facebook-Urteil sagt



#AllFacebook.de
Social Media für Unternehmen

Home + Themen + #AFBMC Konferenz Workshops + 1



Der EUGH hat entschieden.

Muss ich jetzt meine Facebook Seite schließen?

EUGH-URTEIL

Fanpage-Betreiber sind mitverantwortlich für Datenschutz

Wer bei Facebook eine Fanseite betreibt, kann den Datenschutz nicht komplett auf den US-Konzern abwälzen. Datenschutzbeauftragte rechnen damit, dass viele Firmen ihre Fan-Seiten nach einem EuGH-Urteil vorläufig schließen werden.

5. Juni 2018, 13:47 Uhr, Friedhelm Greis



DATENSCHUTZ IM ALLTAG

Was Betreiber von Facebook-Fanseiten beachten müssen

VON MARCUS JUNG UND BASTIAN BENRATH - AKTUALISIERT AM 05.06.2018 - 18:16

online

Online

Websuche mit Google



IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft

EuGH-Urteil

Fanpage-Betreiber sind für Datenschutz mitverantwortlich

05.06.2018, 16:33 Uhr | Alkimos Sartoros, dpa



Facebook: Wer eine Fanseite auf dem sozialen Netzwerk betreibt, ist für den Datenschutz seiner Fans mitverantwortlich. (Quelle: Matt Rourke/AP/dpa)



TOPTHEMEN: CEBIT DSGVO WINDOWS 10 ANDROID P KRYPTOWÄHRUNG ELEKTROAUTOS

heise online > News > 06/2018 > EuGH: Betreiber von Facebook-Fanseiten sind für Datenschutz...

EuGH: Betreiber von Facebook-Fanseiten sind für Datenschutz mitverantwortlich

05.06.2018 14:26 Uhr - Christiane-Schulzki Haddouti

vorlesen



SOCIAL MEDIA

16. → Social Media-Pages ("Fanpages")

Wir unterhalten öffentlich zugängliche Profile bei den Social-Media-Netzwerken YouTube, LinkedIn und Xing („Social-Media-Pages“ oder „Fanpages“).

Wenn Sie eine unserer Social-Media-Pages besuchen und bei dem jeweiligen Social-Media-Netzwerk eingeloggt sind, kann der Anbieter des jeweiligen Social-Media-Netzwerks Ihr Nutzungsverhalten analysieren und die dabei erhobenen Informationen Ihrem Account bei dem Social-Media-Netzwerk zuordnen und diese dort anreichern. Auch wenn Sie nicht eingeloggt sind oder wenn Sie gar keine Account bei dem jeweiligen Social-Media-Netzwerk haben, können Daten zu Ihrer Person von dem Anbieter des jeweiligen Social-Media-Netzwerks erhoben werden, beispielsweise Ihre IP-Adresse oder Daten, die über ein Cookie erhoben werden.

Die Betreiber der Social-Media-Netzwerke können anhand dieser Daten Nutzerprofile erstellen. Anhand Ihres Nutzerprofils können Ihnen dann sowohl auf den Websites des Social-Media-Netzwerks als auch auf anderen Websites interessenbasierte Werbeanzeigen angezeigt werden.

Wenn Sie eine unserer Social-Media-Pages besuchen, sind wir gemeinsam mit dem Anbieter des Social-Media-Netzwerks verantwortlich für die dort stattfindende Erhebung und Verarbeitung Ihrer personenbezogenen Daten. Hinsichtlich der Information über die dort stattfindende Erhebung und Verarbeitung Ihrer personenbezogenen Daten verweisen wir Sie auf die Datenschutzzinformationen der Social-Media-Netzwerke. Weitergehende Informationen liegen uns dazu nicht vor. Die Datenschutzzinformationen der Social-Media-Netzwerke finden Sie hier:

YouTube: https://support.google.com/youtube/topic/2803240?hl=de&ref_topic=6151248

LinkedIn: <https://www.linkedin.com/legal/privacy-policy>

Xing: <https://www.xing.com/privacy>

Informationen zu den geeigneten Garantien für die Datenübermittlung in Drittländer gemäß Art. 46 DSGVO stellen wir Ihnen auf Anfrage jederzeit gerne zur Verfügung.

Ihre Betroffenenrechte gemäß Kapitel III. der DSGVO (Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit etc.) können Sie sowohl gegenüber uns als auch gegenüber dem Anbieter des jeweiligen Social-Media-Netzwerks geltend machen. Wir weisen in diesem Zusammenhang darauf hin, dass wir die Verarbeitung personenbezogener Daten und die Umsetzung der Betroffenenrechte im Rahmen unserer Social-Media-Pages nur im Rahmen der uns von dem jeweiligen Anbieter zur Verfügung gestellten Möglichkeiten beeinflussen können.

Christian Schmoll

Es gab da kürzlich ein EuGH-Urteil, in dem, kurz gesagt, festgestellt wurde, dass Sie als Betreiber einer solchen Page bei einem sozialen Netzwerk mitverantwortlich sind für die dort stattfindende Datenverarbeitung. Damit hat man nun ein gewisses rechtliches Risiko, wenn man so eine Page anbietet, vor allem deswegen, weil man nicht genau weiß, was Facebook, Google etc. da eigentlich genau mit den Daten treiben. Wenn man auf Nummer Sicher gehen will, schaltet man natürlich die Pages jetzt erstmal ab, wozu ich als Anwalt, der verpflichtet ist, immer den sichersten Weg aufzuzeigen, natürlich erst mal raten muss. Ich denke aber, dass es sich hier durchaus um ein vertretbares Risiko handelt, dass man aber versuchen kann, dieses Risiko noch zu reduzieren, indem man diese „Pseudo-Datenschutzerklärung“ zu den Pages hier, die letzten Endes natürlich nichts anders macht, als auf die Datenschutzzinfos der sozialen Netzwerke zurückzuverweisen, auf den Social-Media-Pages verlinkt.



- **Datenminimierung**
- **Informationspflichten (Antrag vs. Förderung)**
- **Aufbewahrung & Löschkonzept**
- **Weitergabe an Dritte („need-to-know“)**
- **Rechtsgrundlage der Weitergabe?**
- **Datensicherheit**
- **Presse/Fotos**

LEGAL BASICS

REAL LIFE PROBLEMS

Q&A



dp.institute

Data Protection Consulting GmbH

Christian Schmoll

Rechtsanwalt, Fachanwalt IT-Recht
CIPP/E, CIPM, FIP, betr. DSB (TÜV)

www.dp.institute

Tel.: 089-4622 7322

schmoll@dp.institute

