

# Information zum Datenschutz

**LovoSoft GmbH**

## Vorwort

Dieses Datenschutzinformationsheft soll Ihnen helfen, sich über das Thema Datenschutz grundlegend zu informieren. Es ist gedacht, vor oder nach einer Datenschutzeschulung bei Fragen zu helfen. Es ist nicht abschließend und natürlich sollten Sie sich bei Fragen, welche über die hier aufgelisteten Punkte hinausgehen, immer einfach direkt an Ihren Datenschutzbeauftragten wenden.

Über Ihre Anregungen / Verbesserungsvorschläge würden wir uns freuen.  
Einfach per E-Mail an: [info@lovosoft.de](mailto:info@lovosoft.de)

Viel Spaß beim Lesen!

T. Volkert

# Inhaltsverzeichnis (1)

<b>1</b>	<b>Übersicht der wichtigsten Fakten</b> .....	<b>1</b>
1.1	Zweck von Datenschutz und der DS-GVO.....	1
1.2	Persönlichkeitsrecht .....	1
1.3	Recht auf informationelle Selbstbestimmung.....	1
1.4	Gesetzliche Regelungen zum Datenschutz.....	1
1.5	Personenbezogene Daten .....	2
1.6	Verarbeitung von Daten .....	2
1.7	Personenbezogene Daten in Unternehmen.....	3
1.8	Weisungsgebundenheit und Verschwiegenheit.....	3
1.9	Rechte des Betroffenen (Art. 12-23 DS-GVO) .....	3
1.10	Aufgaben des Datenschutzbeauftragten (Art. 39 DS-GVO).....	4
1.11	Einführung neuer Datenverarbeitungsverfahren.....	4
1.12	Einsatz von Videoüberwachung .....	4
1.13	Verarbeitung von Beschäftigtendaten (Art. 88 DS-GVO) .....	4
1.14	Datenschutzverstöße (Art. 83 DS-GVO) .....	5
1.15	Folgen für das Unternehmen .....	5
1.16	Arbeitsrechtliche Konsequenzen bei Daten- schutzverstößen .....	5
<b>2</b>	<b>Was steckt hinter dem Datenschutz</b> .....	<b>6</b>
2.1	Zweck von Datenschutz und der DS-GVO.....	6
2.2	Definition des Persönlichkeitsrechts .....	6
2.3	Was genau gehört zur informationellen Selbstbestimmung?.....	6
2.4	Die Verordnung (EU) 2016/2679 des europäischen Parlaments und des Rates .....	6
2.5	Datenschutzgesetze, die ein Unternehmen berücksichtigen muss .....	7
2.6	Definition personenbezogener Daten .....	7
2.7	Welche Daten schützt die DS-GVO? .....	7
2.8	Erfasst die DS-GVO auch Firmendaten? .....	8
2.9	Schützt die DS-GVO auch im privaten Umfeld?.....	8
2.10	Erfasst die DS-GVO auch den Datenverkehr mit Papier und Bleistift?.....	8
2.11	Was bedeutet nicht automatisierte Verarbeitung? .....	8
2.12	Unterschiedliche personenbezogene Daten .....	8
<b>3</b>	<b>Verarbeiten von personenbezogenen Daten</b> .....	<b>10</b>
3.1	Was versteht man unter Verarbeitung von Daten? .....	10
3.2	Was benötigt man um personenbezogene Daten verarbeiten zu dürfen?.....	11
3.3	Was ist eine Einwilligung? .....	12
3.4	Ab wann ist die Einwilligung wirksam erteilt?.....	12
3.5	Welche Kriterien sollte eine Einwilligungs- erklärung optisch aufweisen?.....	13
3.6	Wie lange gilt eine Einwilligungserklärung?.....	13
3.7	Wie alt muss man sein, um eine Einwilligungserklärung abgeben zu können? .....	13
3.8	Einwilligungserklärungen im Internet .....	14
3.9	Verarbeitung personenbezogener Daten ohne Einwilligung .....	14
<b>4</b>	<b>Die DS-GVO im Unternehmen</b> .....	<b>16</b>
4.1	Welche personenbezogenen Daten werden in einem Unternehmen geschützt? .....	16
4.2	Kontrolliert der Staat das Einhalten der DS- GVO? .....	16
4.3	Verantwortliche für die Einhaltung des Datenschutzes in einem Unternehmen .....	17
4.4	Kontrolle des Datenschutzes im Unternehmen .....	17
4.5	Sollten Mitarbeiter eine Verpflichtungs- erklärung unterschreiben? .....	17
4.6	Geltung der Verpflichtung .....	18
4.7	Rechte des Betroffenen.....	18
4.8	Transparente Information und Kommunikation (Art.12 DS-GVO) .....	18
4.9	Hat der Betroffene das Recht auf Informationen (aktive Informationen)? .....	19

4.10	Hat der Betroffene ein Recht auf Auskunft (reaktive Information)?	21
4.11	Hat man das Recht auf Berichtigung?	22
4.12	Hat der Betroffene das Recht auf Löschung seiner Daten? (Art. 17 DS-GVO)	22
4.13	Hat man das Recht auf Einschränkung? (Art. 18 DS-GVO)	23
4.14	Hat man das Recht auf eine Mitteilung im Zusammenhang mit der Berichtigung oder der Einschränkung der Verarbeitung? (Art. 19)	24
4.15	Hat man das Recht auf Datenübertragbarkeit? (Art. 20 DS-GVO)	25
4.16	Hat man das Recht auf Widerspruch? (Art. 21 DS-GVO)	26
4.17	Hat man das Recht auf nicht ausschließlich automatisierte Entscheidungen?	26
4.18	Hat man das Recht auf Beschwerde bei einer Aufsichtsbehörde?	27
4.19	Hat man das Recht einen Datenschutzbeauftragten zu konsultieren?	27
<b>5</b>	<b>Verarbeitung von Daten durch externe Dienstleister</b>	<b>28</b>
5.1	Beauftragung anderer Unternehmen mit personenbezogenen Daten	28
5.2	Was genau muss bei der Auftragsdatenverarbeitung festgelegt werden?	28
5.3	Dokumentation darf nicht vergessen werden	29
5.4	Geltung der Bestimmungen zur Auftragsverarbeitung, wenn Verarbeitung nicht im Vordergrund steht	29
5.5	Wer ist zu informieren, wenn Tätigkeiten ausgelagert werden?	29
<b>6</b>	<b>Datenaustausch innerhalb des Unternehmensverbundes</b>	<b>31</b>
6.1	Was ist zu beachten, wenn Daten zwischen Unternehmen im Konzern oder Unternehmensverbund ausgetauscht werden sollen?	31
6.2	Zu welchem Zeitpunkt dürfen Daten zwischen verbundenen Unternehmen ausgetauscht werden?	31
<b>7</b>	<b>Der Datenschutzbeauftragte (DSB)</b>	<b>32</b>
7.1	Ab wann braucht ein Unternehmen einen Datenschutzbeauftragten?	32
7.2	Aufgaben des Datenschutzbeauftragten	33
7.3	Sollte der Datenschutzbeauftragte bei neuen Datenverarbeitungsverfahren informiert werden?	34
<b>8</b>	<b>Verstöße und Pannen des Datenschutzes</b>	<b>35</b>
8.1	Welche Folgen hat ein Verstoß beim Datenschutz?	35
8.2	Wer muss informiert werden, wenn eine Verletzung des Datenschutzes entstanden ist?	36
8.3	Kann eine Verletzung auch arbeitsrechtliche Konsequenzen haben?	36
8.4	Schadensersatz für betroffene Personen	37
8.5	Sollten dem Datenschutzbeauftragten Verstöße gemeldet werden?	37
<b>9</b>	<b>Unternehmen mit Videoüberwachung</b>	<b>39</b>
9.1	Welche Regelungen müssen bei der Videoüberwachung eingehalten werden?	39
9.2	Gibt es Vorschriften außerhalb der DS-GVO zur Videoüberwachung?	39
9.3	Unterschied zwischen öffentlich zugänglichen und nicht öffentlich zugänglichen Räumen	39
9.4	Gibt es einen Unterschied ob Bilddaten gespeichert werden oder nicht?	40
9.5	Darf heimlich videoüberwacht werden?	40
9.6	Dürfen bestimmte Bereiche nicht videoüberwacht werden?	40
9.7	Wer prüft die Zulässigkeit einer Videoüberwachung?	40
<b>10</b>	<b>Datenverarbeitung im Beschäftigungsverhältnis</b>	<b>41</b>
10.1	Welche Regelungen gibt es für den Umgang mit Beschäftigtendaten im Unternehmen?	41
10.2	Beschäftigte eines Unternehmens	41
10.3	Wann darf ein Unternehmen personenbezogene Daten seiner Beschäftigten verarbeiten?	42
10.4	Dürfen personenbezogene Daten von einem Unternehmen verarbeitet werden um Straftaten aufzudecken?	42
10.5	Muss die Mitarbeitervertretung dem Verfahren zustimmen?	42
<b>11</b>	<b>Datenschutz am Arbeitsplatz</b>	<b>44</b>

11.1 Einhalten des Clean-Desk-Prinzips .....	44
11.2 Sollte bei Passwörtern Mindestanforderungen beachtet werden? .....	45
11.3 Aufbewahrung von Passwörtern .....	46
11.4 Sollten Passwörter Kollegen gegeben werden? .....	46
11.5 Entsorgen von Unterlagen.....	46
11.6 Was muss bei der Entsorgung von Datenträgern beachtet werden? .....	47
11.7 Umgang mit Besuchern und Gästen.....	47
<b>12 Datenschutz unterwegs.....</b>	<b>48</b>
12.1 Anwendung des Minimalprinzips .....	48
12.2 Aufbewahrung von Notebooks, Datenträgern und Unterlagen unterwegs.....	48
12.3 Verschlüsselung von Datenträgern und Daten.....	49
12.4 E-Mail-Verschlüsselung .....	49
12.5 Besonders bedeutende Schutzmechanismen .....	49
12.6 Arbeit im Zug, Flugzeug und Hotellobby .....	49
12.7 Welches WLAN sollte für die Verbindung ins Internet genutzt werden? .....	50
12.8 Gestohlene Computer, Datenträger oder Unterlagen .....	50
12.9 Bring your own device (BYOD) .....	50
12.10 Homeoffice.....	50
12.11 Private Nutzung.....	51
<b>13 Anlagen .....</b>	<b>1</b>
13.1 Wer trägt in einem Unternehmen die Verantwortung .....	1
13.2 Rechte der betroffenen Person .....	2
13.3 personenbezogene Daten .....	8
13.4 Richtigkeit der Verarbeitung .....	9
13.5 Die Einwilligung .....	9
13.6 Datenschutz im Unternehmen .....	10
13.7 Gültigkeit der Verpflichtung auf Verschwiegenheit .....	10
13.8 Rechte der betroffenen Person .....	10
13.9 Schritte der Verarbeitung.....	11
13.10 Datenfluss und Tätigkeiten bei der Auftragsdatenverarbeitung Bsp. ....	11
13.11 Aufgaben des Datenschutzbeauftragten .....	11
13.12 Allgemeine Bedingungen für die Verhängung von Geldbußen Art 83.....	12
13.13 Prozess beim Entdecken von Verstößen.....	12
13.14 Clean-Desk-Prinzip .....	12
13.15 Wer trägt die Konsequenzen?.....	13
13.16 Mindestanforderungen bei der Passwortwahl .....	13
13.17 Datenschutz unterwegs .....	14

# 1 Übersicht der wichtigsten Fakten

## 1.1 Zweck von Datenschutz und der DS-GVO

Der Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, durch den Umgang mit personenbezogenen Daten in seinem Recht oder seiner Freiheit, besonders in seinem Persönlichkeitsrecht, beeinträchtigt zu werden.

## 1.2 Persönlichkeitsrecht

Das allgemeine Persönlichkeitsrecht findet sich in der Charta der Grundrechte der Europäischen Union (Art. 7 und 8) und im Grundgesetz der Bundesrepublik Deutschland (Art. 2 Abs. 1 GG). Jeder Einzelne hat das Recht auf:

- Individualsphäre (Schutz des Selbstbestimmungsrechts)
- Privatsphäre (Leben im häuslichen Bereich, Privatleben)
- Intimsphäre (innere Gedanken- und Gefühlswelt)

## 1.3 Recht auf informationelle Selbstbestimmung

Dies ist das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

## 1.4 Gesetzliche Regelungen zum Datenschutz

- Datenschutz-Grundverordnung (DS-GVO)
- „BDSG-neu“ (DSAnpUG-EU / BDSG n.F.)
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Sozialgesetzbücher (SGB)
- Landesdatenschutzgesetz (LDSG)
- Regelung der katholischen und evangelischen Kirche
- Und weitere.

Die verantwortliche Stelle muss sich gesetzeskonform verhalten.

## 1.5 Personenbezogene Daten

Dies sind alle Informationen über eine identifizierte oder identifizierbare natürliche Person, die sogenannte betroffene Person. Hierbei handelt es sich um Einzelangaben zu persönlichen oder sachlichen Verhältnissen der betroffenen Personen.



## 1.6 Verarbeitung von Daten

Zu der Verarbeitung gehört das Erheben, Erfassen, Organisieren und Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen oder Verwenden, Übermitteln, die Verbreitung oder eine andere Form der

Bereitstellung, der Abgleich oder die Verknüpfung, Einschränkung, Löschen und Vernichten von personenbezogenen Daten.

**Grundsätzlich ist die Verarbeitung von personenbezogenen Daten verboten.** Jedoch ist es **erlaubt**, wenn es aus der **DS-GVO**, **einer anderen Rechtschrift** oder **einer Einwilligung** des Betroffenen hervorgeht.

## 1.7 Personenbezogene Daten in Unternehmen

- Daten der Mitarbeiter
- Daten der Bewerber
- Daten von Kunden
- Daten von Lieferanten

## 1.8 Weisungsgebundenheit und Verschwiegenheit

Bei der Verarbeitung von personenbezogenen Daten muss der Verantwortliche sicherstellen, dass die mit der Datenverarbeitung beschäftigten Personen ausschließlich auf dessen Weisung hin und im Einklang mit den gesetzlichen Regelungen personenbezogene Daten verarbeiten. Die Verpflichtung wird aus Nachweisgründen schriftlich vorgenommen. Die Verpflichtung und Verschwiegenheit gilt nicht nur während der Ausübung ihrer Tätigkeit für das Unternehmen, sondern auch nach Ende Ihrer Beschäftigung. Dies bedeutet, dass danach eine unberechtigte Verarbeitung von personenbezogenen Daten verboten ist.

## 1.9 Rechte des Betroffenen (Art. 12-23 DS-GVO)

- Das Recht auf transparente Information und Kommunikation
- Das Recht auf Auskunft über personenbezogene Daten
- Das Recht auf Berichtigung von personenbezogenen Daten
- Das Recht auf Löschung (Vergessenwerden von personenbezogenen Daten)
- Das Recht auf Einschränkung von personenbezogener Daten
- Das Recht auf Widerspruch
- Das Recht auf Datenübertragbarkeit
- Das Recht auf nicht ausschließlich automatisierte Entscheidungen
- Das Recht auf Beschwerde bei einer Aufsichtsbehörde
- Das Recht, den Datenschutzbeauftragten zu konsultieren



## 1.10 Aufgaben des Datenschutzbeauftragten (Art. 39 DS-GVO)

- Überwachung der Einhaltung der DS-GVO und anderen Vorschriften zum Datenschutz
- Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme
- Schulung der Mitarbeiter im Datenschutz
- Beratung der Unternehmensleitung und der Mitarbeiter im Umgang mit personenbezogenen Daten
- Anlaufstelle für Aufsichtsbehörden für den Datenschutz und für die betroffenen Personen
- Auskunftserteilung, wie mit Daten im Unternehmen umgegangen wird

**1.11 Einführung neuer Datenverarbeitungsverfahren**  
Der betriebliche Datenschutzbeauftragte muss ordnungsgemäß und frühzeitig über diese Vorhaben zur Einführung neuer Datenverarbeitungsverfahren informiert werden.

## 1.12 Einsatz von Videoüberwachung

- Bei öffentlich zugänglichen Bereichen gelten die Regelungen in Art. 6 und 35 DS-GVO und §4 DSAnpUG-EU.
- Bei nicht öffentlich zugänglichen Bereichen im Beschäftigungsverhältnis ist §26 DSAnpUG-EU die einschlägige Rechtsgrundlage.

## 1.13 Verarbeitung von Beschäftigtendaten (Art. 88 DS-GVO)

Art. 88 DS-GVO erlaubt nationale Rechtsvorschriften zur personenbezogenen Beschäftigtendaten im Beschäftigungskontext. Daher gilt in Deutschland:

- Gemäß § 26 DSAnpUG-EU dürfen personenbezogene Daten von Beschäftigten verarbeitet werden, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.
- Zur Ermittlung von Straftaten dürfen unter bestimmten Bedingungen personenbezogene Daten der Beschäftigten erhoben, verarbeitet oder genutzt werden.

## 1.14 Datenschutzverstöße (Art. 83 DS-GVO)

Wenn unrechtmäßigerweise personenbezogene Daten verarbeitet werden oder Anforderungen der DS-GVO nicht umgesetzt werden, so wird gegen die DS-GVO verstoßen.

## 1.15 Folgen für das Unternehmen

- Je nach Tatbestand können Geldbuße von bis zu 20.000.000 € oder bis zu 4 % des gesamt weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welche der Beträge höher ist, drohen.
- „Datenschutzpannen“ können nachhaltig das Ansehen des Unternehmens beeinträchtigen.

## 1.16 Arbeitsrechtliche Konsequenzen bei Datenschutzverstößen

- Das Unternehmen kann den Ersatz des entstandenen Schaden vom Arbeitnehmer verlangen, wenn der Verstoß absichtlich oder grob fahrlässig verursacht wurde.
- Eine Verletzung datenschutzrechtlicher Bestimmungen kann zu einer arbeitsrechtlichen Abmahnung führen.
- Sollte es dem Unternehmen nicht mehr zumutbar sein, den Arbeitnehmer weiter zu beschäftigen, so kann das Unternehmen eine Kündigung aussprechen.

## 2 Was steckt hinter dem Datenschutz

### 2.1 Zweck von Datenschutz und der DS-GVO

Die DS-GVO regelt den Umgang mit personenbezogenen Daten. Hierbei wird beachtet das Recht auf Achtung des Privat- und Familienlebens nicht zu verletzen. Unter anderen schützt die DS-GVO die Grundrechte und Grundfreiheiten natürlicher Personen insbesondere das Recht auf Schutz personenbezogener Daten. Somit schützt sie die natürlichen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten.

### 2.2 Definition des Persönlichkeitsrechts

Im Allgemeinen ist das Persönlichkeitsrecht in dem Grundgesetz bestimmt (Art. 2 Abs. 1 GG). Durch eben diese Regelung gibt es jedem das Recht auf Individualsphäre, was so viel bedeutet wie der Schutz der Selbstbestimmung, also das Recht auf informationelle Selbstbestimmung. Das Persönlichkeitsrecht gibt auch das Recht auf Privatsphäre, wie das Leben im häuslichen Bereich bzw. das Privatleben abläuft. Die inneren Gedanken und die Gefühlswelt einer Person (Intimsphäre) sind ebenfalls Teil des Persönlichkeitsrechts.

### 2.3 Was genau gehört zur informationellen Selbstbestimmung?

Die informationelle Selbstbestimmung ist Teil des allgemeinen Persönlichkeitsrechts. Es gibt der einzelnen Person das Recht selbst zu bestimmen welche seiner personenbezogenen Daten preisgegeben und verwendet werden dürfen. Somit kann z.B. selbst entschieden werden ob Informationen über einen im Internet veröffentlicht werden oder nicht. Sollten allerdings gegen den Willen einer Person Daten über diese veröffentlicht werden, so kann dieser dagegen vorgehen, da sie in ihrem Recht der informationellen Selbstbestimmung verletzt wurde.

### 2.4 Die Verordnung (EU) 2016/2679 des europäischen Parlaments und des Rates

Dies ist das wichtigste Gesetz, welches Auskunft über den Umgang mit personenbezogenen Daten gibt. Kurz nennt man diese Verordnung die Datenschutz-Grundverordnung (DS-GVO). Sie ist ein vorrangiges Gesetz,

welches vor allen nationalen gesetzlichen Regelungen gilt, da es sich um eine EU-Verordnung handelt.

Durch nationale Regelungen darf die DS-GVO lediglich spezifiziert, konkretisiert oder ergänzt werden unter der Bedingung, dass die DS-GVO dies zulässt. Es gibt allerdings auch andere Gesetze, welche Vorgaben für den Umgang mit personenbezogenen Daten machen. Das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG) oder Sozialgesetzbüchern (SGB) sind Beispiele dafür, wo ebenfalls für Datenschutz gesorgt wird. In Katholischer und Evangelischer Kirche gibt es ebenfalls Regelung zum Datenschutz, welche mit der DS-GVO im Einklang stehen. Der Umgang mit personenbezogenen Daten ist in einem Unternehmen beispielsweise durch eine Betriebsvereinbarung geregelt.

## 2.5 Datenschutzgesetze, die ein Unternehmen berücksichtigen muss

In wie weit ein Unternehmen alle Datenschutzgesetze einhalten muss hängt davon ab, wie das einzelne Unternehmen organisiert ist. Die DS-GVO gilt Grundsätzlich für alle privatrechtlichen Unternehmen. Kindergärten und Kirchengemeinden fallen allerdings unter das kirchliche Datenschutzrecht. Die Regelungen der DS-GVO gelten auch für öffentliche Stellen, wie z.B. die Stadtverwaltung.

## 2.6 Definition personenbezogener Daten

Unter personenbezogenen Daten versteht man z.B. den Namen, Adresse, Telefonnummer, Geburtsdatum, Foto, E-Mail-Adresse, Arbeitsverhalte, Kfz-Kennzeichen, Gesundheitsinformation und andere Informationen einer einzelnen natürlichen Person. Sollten die Informationen allerdings keine eindeutige Zuordnung zu einer einzelnen natürlichen Person herstellen können, so fällt die Verarbeitung solcher Daten nicht unter die DS-GVO.

## 2.7 Welche Daten schützt die DS-GVO?

Nur personenbezogene Daten fallen in den Anwendungsbereich der DS-GVO. Was unter personenbezogenen Daten zu verstehen ist legt die DS-GVO genau fest. Dazu gehören alle Informationen über **eine identifizierte oder identifizierbare natürlich Person**, die sogenannte **betroffene Person**. Wenn einzelne Informationen oder das Kombinieren der einzelnen Informationen dazu führen, dass man Rückschlüsse auf die natürliche Identität der betroffenen Person ziehen könnte, so ist diese Identifizierbar.

## 2.8 Erfasst die DS-GVO auch Firmendaten?

Juristische Personen (AG, GmbH oder GmbH & Co. KG) werden mit ihren Daten von der DS-GVO nicht erfasst. Ein Unternehmen welches aus einer Personengesellschaft besteht wird von der DS-GVO erfasst, da es sich hier um natürliche Personen handelt. Beispiele für Personengesellschaften sind Malerfachgeschäfte oder Metzger. Unter die Bestimmung der DS-GVO fallen ebenfalls die personenbezogenen Daten der Ansprechpartner einer AG oder GmbH. Sollte es sich um eine Ein-Personen-GmbH handeln, so fallen die personenbezogenen Daten dieser ebenfalls unter die Vorgaben der DS-GVO, obwohl es sich um eine Kapitalgesellschaft handelt.

## 2.9 Schützt die DS-GVO auch im privaten Umfeld?

Wenn personenbezogene Daten **ausschließlich für persönliche und familiäre Tätigkeiten** verwendet oder verarbeitet werden so fällt dies **nicht** unter die Vorgaben der DS-GVO.

## 2.10 Erfasst die DS-GVO auch den Datenverkehr mit Papier und Bleistift?

Die Verarbeitung elektronisch erfassten Daten ist zwar einfacher, bedeutet jedoch nicht das die Datenverarbeitung von Papier nicht auch von der DS-GVO erfasst wird. Die personenbezogenen Daten sollten unabhängig von der verwendeten Technik geschützt werden. Unter automatisierter Verarbeitung versteht man, wenn personenbezogenen Daten unter Einsatz von Datenverarbeitungsanlagen erhoben, verarbeitet oder genutzt werden.

## 2.11 Was bedeutet nicht automatisierte Verarbeitung?

Unter nicht automatisierter Verarbeitung versteht man die Verarbeitung, Erhebung und Nutzung ohne die Hilfe von Datenverarbeitungs-Anlagen (Personal-Datenbanken, Lieferanten-Daten, ERP Systeme).

## 2.12 Unterschiedliche personenbezogene Daten

Es gibt personenbezogene Daten, welche besonders schützenswert sind. Nur unter bestimmten Voraussetzungen dürfen diese verarbeitet werden. In Art. 9 (1) der DS-GVO ist festgelegt welche Daten darunter fallen.

Zu den **besonders schützenswerten personenbezogenen Daten (besondere Kategorien pd Daten)** gehört die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Verarbeitung von genetischen Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

## 3 Verarbeiten von personenbezogenen Daten

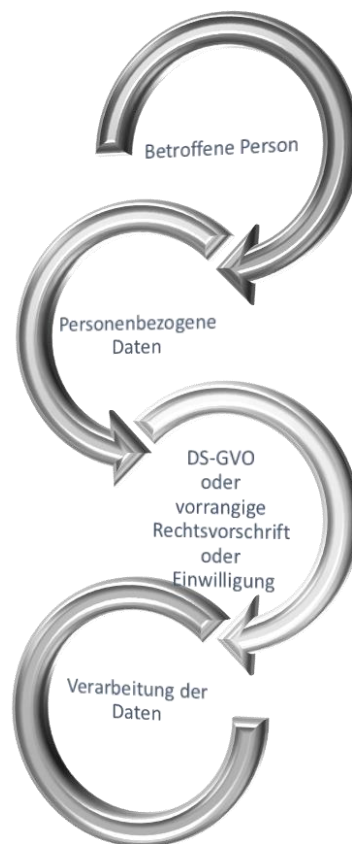
### 3.1 Was versteht man unter Verarbeitung von Daten?

Der Begriff „Verarbeiten“ umfasst in der DS-GVO eine Vielzahl von Tätigkeiten, die an oder mit personenbezogenen Daten durchgeführt werden. Diese Tätigkeiten heißen:

- **Erheben** - Daten der natürlichen Person (der Betroffene) beschaffen
- **Erfassen** - erfasste Daten überführen in ein relevantes Dateisystem
- **Organisieren** und **Ordnen** - Zuordnen von Sortier- und Suchkriterien, sowie deren geordnete Verwendung im Dateisystem
- **Speichern** - personenbezogene Daten erfassen, aufnehmen oder aufbewahren auf einem Datenträger, um diese zu nutzen oder weiterzuverarbeiten
- **Anpassen** oder **Verändern** - gespeicherte personenbezogene Daten inhaltlich umgestalten
- **Auslesen, Abfragen** oder **Verwenden** - gespeicherte personenbezogene Daten darstellen oder nutzen
- **Übermitteln, Verarbeiten** oder andere Form der **Bereitstellung** - durch Datenverarbeitung gewonnene personenbezogene Daten oder die Weitergabe gespeicherter personenbezogener Daten an einen Dritten.
- **Abgleich** oder **Verknüpfung** - anhand eindeutiger Kriterien personenbezogene Daten vergleichen, verknüpfen oder zusammenführen
- **Einschränken** - um weitere Verarbeitung bzw. Nutzung von gespeicherten personenbezogenen Daten zu sperren, müssen diese gekennzeichnet werden
- **Löschen** - gespeicherte personenbezogene Daten nicht wieder herstellbar entfernen
- **Vernichten** - nicht automatisierte personenbezogene Daten bzw. von Datenträgern, auf welchen personenbezogene Daten gespeichert sind, nicht wiederherstellbar vernichten

## 3.2 Was benötigt man um personenbezogene Daten verarbeiten zu dürfen?

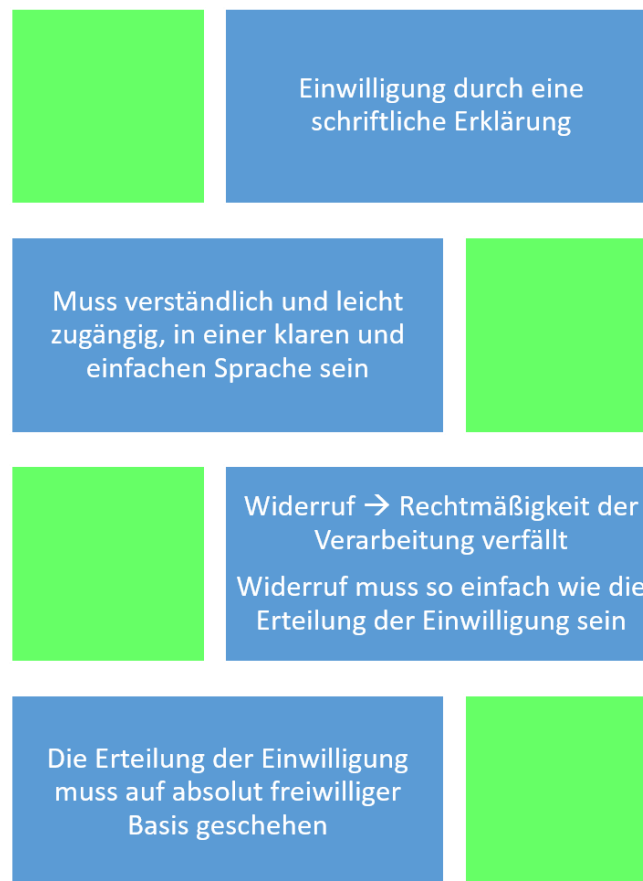
Durch das „**Erlaubnisvorbehaltsprinzip**“ ist die DS-GVO geprägt. Laut diesem Prinzip ist die Verarbeitung von personenbezogener Daten **grundsätzlich verboten**, außer es liegt eine entsprechende **Rechtsgrundlage** vor. Durch die DS-GVO oder einer anderen (vorrangigen) Rechtsvorschrift oder der **Einwilligung** des Betroffenen kann sich dies ergeben.





### 3.3 Was ist eine Einwilligung?

Um seinen freien Willen Ausdruck zu verleihen, erteilt der Betroffene eine sogenannte Einwilligung, in welcher er sich einverstanden erklärt, dass seine personenbezogenen Daten für einen bestimmten Zweck verarbeitet werden dürfen. Die **Einwilligung muss vor dem Beginn der Verarbeitung** erfolgen.



### 3.4 Ab wann ist die Einwilligung wirksam erteilt?

Eine Einwilligung kann laut der DS-GVO (Art. 7) und den dazugehörigen Erwägungsgründen nur unter bestimmten Voraussetzungen für wirksam erklärt werden. Diese Voraussetzungen wären:

- Die Einwilligung erfolgt **freiwillig**
- Sie sollte **nicht** mit anderen Einwilligungen **gekoppelt** werden und nur für einen konkreten Fall bestimmt sein
- Für die betroffene Person muss die Einwilligung klar und verständlich formuliert sein
- Der Zweck der Datenverarbeitung muss erkennbar sein
- Sollten unterschiedliche Verarbeitungszwecke vorliegen sind mehrere Einwilligungen abzugeben

- Die einwilligende Person muss über ihre Widerrufsmöglichkeit unterrichtet werden
- Sie muss durch eine eindeutige aktive Handlung erfolgen. Sollte die Einwilligung also vorgegeben sein und der Betroffene müsste durch Durchstreichen oder entfernen eines Häkchens quasi erst seine Einwilligung verneinen so ist diese unwirksam.
- Die Einwilligung muss der Verarbeitende vorweisen können

### 3.5 Welche Kriterien sollte eine Einwilligungserklärung optisch aufweisen?

Für eine geltende Einwilligungserklärung muss folgendes beachtet werden:

- Sie darf nicht versteckt sein.
- Bei einer zusammenhängenden Erklärung muss sie optisch hervorgehoben werden, z.B. ist dem Betroffenen nicht klar, dass er eingewilligt hat, wenn die Einwilligungserklärung in den Allgemeinen Geschäftsbedingungen versteckt ist.

### 3.6 Wie lange gilt eine Einwilligungserklärung?

Das besondere bei Einwilligungserklärungen zum Umgang mit personenbezogenen Daten ist, dass diese jederzeit widerrufen werden können. Sollte der Betroffene also seine Einwilligungserklärung zurückziehen, so ist die Verarbeitung seiner personenbezogenen Daten für die Zukunft nicht mehr gestattet. Eine Verarbeitung personenbezogener Daten ohne die Einwilligung des Betroffenen ist unzulässig.

### 3.7 Wie alt muss man sein, um eine Einwilligungserklärung abgeben zu können?

Minderjährige, die bei einem Angebot von Diensten der Informationsgesellschaft einwilligen möchte, müssen das 16. Lebensjahr, nach den Vorgaben der DS-GVO, beendet haben, um die Einwilligung geltend zu machen. Für Minderjährige, die das 16. Lebensjahr noch nicht beendet haben, ist die Einwilligung von allen Sorgeberechtigten einzuholen. Andere EU-Mitgliedsstaaten können allerdings per Rechtsvorschrift eine niedrigere Altersgrenze festlegen, welche jedoch mindestens das vollendete 13. Lebensjahr voraussieht. Dass die Folgen seines Handelns abgeschätzt werden können, wird von einem 14-jährigen erwartet. Ob jemand jetzt wirklich einsichtsfähig ist, hängt jedoch von vielem ab, z.B.:

- Sachverhalte, welche kompliziert und schwer zu erfassen sind
- Es ist nötig, dass die einwilligende Person Erfahrungen im Bereich des Geschäftslebens hat
- Die Umstände der Einwilligungserklärung, also wann, wie und wo, müssen erklärt werden
- Sollten Unsicherheiten entstehen, ist es empfehlenswert eine zusätzliche Einwilligung eines Erziehungsberechtigten einzuholen

### 3.8 Einwilligungserklärungen im Internet

Im Internet lässt sich ohne die Angaben von personenbezogenen Daten kaum ein Vorhaben abwickeln, wie z.B. bei Bestellungen, Gewinnspielen, Abonnieren eines E-Mail-Newsletters. Damit diese Vorhaben abgewickelt werden können, braucht ein Unternehmen die Einwilligung zur Verarbeitung personenbezogener Daten. Jedoch lässt sich nur sehr umständlich eine schriftliche Einwilligung einholen. Um eben diesen ganzen Vorgang zu vereinfachen, hat der Gesetzgeber in verschiedenen anderen Gesetzen, wie z.B. im Telemediengesetz, Regelungen zur elektronischen Einwilligung gegeben. Diese Regelungen lauten:

- Die Einwilligungserklärung muss deutlich und bewusst abgegeben werden.
- Es muss jederzeit der Einwilligungstext aufrufbar sein und die Einwilligungserklärung widerrufbar sein, deshalb sollte darauf geachtet werden, dass diese Einwilligung systemseitig protokolliert wird.

Die Einwilligung muss jederzeit einlesbar für den Betroffenen sein. Außerdem muss der Betroffene die Möglichkeit haben zu jedem Zeitpunkt seine Einwilligung zurück zu ziehen.

### 3.9 Verarbeitung personenbezogener Daten ohne Einwilligung

In der DS-GVO ist die Verarbeitung von Daten so geregelt, dass man hierfür eine Einwilligung des Betroffenen braucht oder aufgrund einer rechtlichen Vorschrift diese nutzen darf. Allerdings wurde in der DS-GVO eine weitere Rechtsgrundlage geschaffen, wobei personenbezogene Daten für einen Geschäftszweck erhoben werden dürfen. Dies ist auch ohne ausdrückliche Einwilligung möglich, wenn

- Diese Daten zur Erfüllung eines Vertrages benötigt werden, wofür vorvertraglich Maßnahmen eingeleitet werden müssen. Dies ist

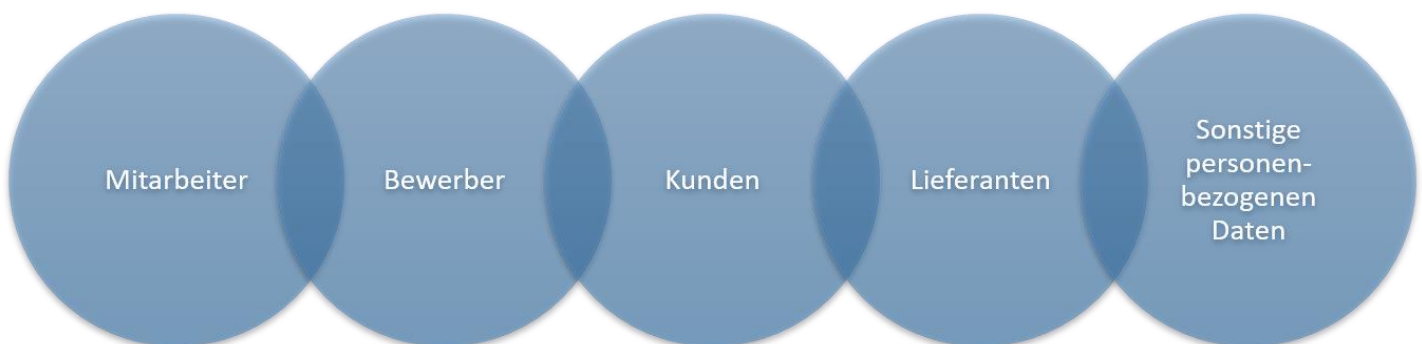
allerdings nur möglich, wenn die betroffene Person eine der Vertragsparteien ist.

- Bei einem Unternehmen, bei dem das berechtigte Interesse an der Nutzung oder Verarbeitung von personenbezogener Daten überwiegt. (ausführlicher in Art. 6 Abs. 1 lit. f beschrieben)

## 4 Die DS-GVO im Unternehmen

### 4.1 Welche personenbezogenen Daten werden in einem Unternehmen geschützt?

Die DS-GVO erfasst alle personenbezogenen Daten, daher sind in einem Unternehmen nicht nur die Daten der Mitarbeiter geschützt, sondern auch die Daten der Bewerber, Kunden oder Lieferanten, sobald eine Verbindung zu einer natürlichen Person hergestellt werden kann.



### 4.2 Kontrolliert der Staat das Einhalten der DS-GVO?

Bestimmte Aufsichtsbehörden kontrollieren das Einhalten des Datenschutzes. Hierfür können diese Behörden von einem Unternehmen eine schriftliche Auskunft zur Verarbeitung personenbezogener Daten verlangen. Um ein Unternehmen zu überprüfen, können die Aufsichtsbehörden allerdings auch unangemeldete Kontrollen vor Ort durchführen. Sollte sich jemand in seinem Persönlichkeitsrecht verletzt sehen, so kann dieser sich an die zuständige Datenschutzaufsichtsbehörde wenden und eine Beschwerde einreichen. Die Aufsichtsbehörde hat dank dem Art. 58 der DS-GVO weitreichende Befugnisse. Diese kann bei schwerwiegenden Verstößen eine Abstellung anordnen, Bußgeld verhängen oder die Verarbeitung von personenbezogenen Daten untersagen.

## 4.3 Verantwortliche für die Einhaltung des Datenschutzes in einem Unternehmen

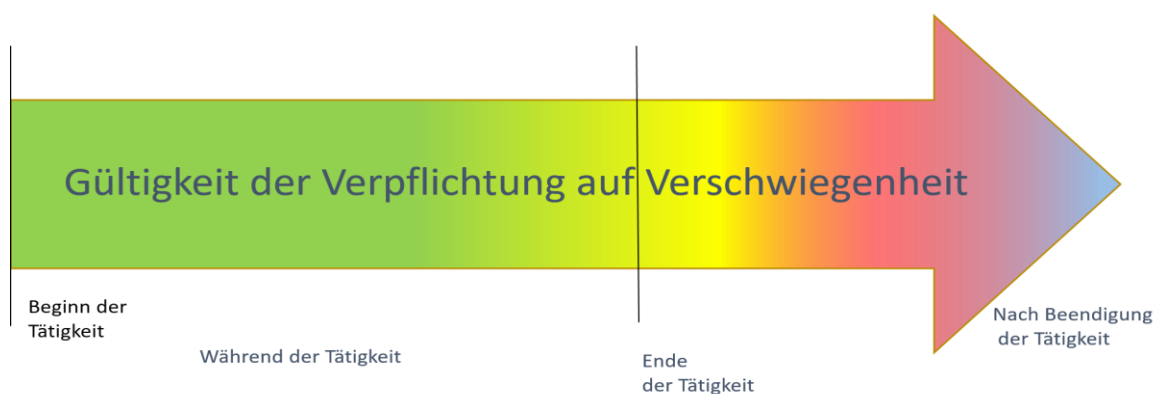
Die Unternehmen tragen Verantwortung für die personenbezogenen Daten, die sie erheben, nutzen oder verarbeiten. So wird das Unternehmen deshalb auch **der Verantwortliche** genannt. Da es sich bei einem Unternehmen meist um eine juristische Person handelt, muss sich die Geschäftsführung um die Einhaltung der DS-GVO kümmern. Auch dadurch, dass die Geschäftsführung das Unternehmen nach außen hin vertritt, ist diese verantwortlich für die Einhaltung des Datenschutzes.

## 4.4 Kontrolle des Datenschutzes im Unternehmen

Der Datenschutzbeauftragte kontrolliert innerhalb eines Unternehmens das Einhalten des Datenschutzes. Seine Aufgabe ist es dafür zu sorgen, dass die Regelungen des Datenschutzes eingehalten werden (Art. 39 DS-GVO Aufgaben des Datenschutzbeauftragten). Der Datenschutzbeauftragte unterstützt damit die Geschäftsführung, welche letztendlich alle erforderlichen Entscheidungen im Hinblick auf die Einhaltung der gesetzlichen Bestimmungen trifft und verantwortet.

## 4.5 Sollten Mitarbeiter eine Verpflichtungserklärung unterschreiben?

Laut Art.29 der DS-GVO ist der Verantwortliche dazu verpflichtet sicher zu stellen, dass die unterstellten Personen, welche Zugang zu personenbezogenen Daten haben, diese **ausschließlich auf Weisung des Verantwortlichen hin verarbeiten dürfen**. Falls nun eine Aufsichtsbehörde einen schriftlichen Nachweis fordert, ist es sinnvoll, dass diese unterstellten Personen einer Verpflichtung schriftlich zugestimmt haben.



## 4.6 Geltung der Verpflichtung

Die Verschwiegenheitsverpflichtung gilt **nicht nur** für den Zeitraum der Tätigkeit für das Unternehmen. Selbst nach Beendigung des Arbeitsverhältnisses ist die **Verschwiegenheitsverpflichtung weiterhin gültig**. Dies bedeutet, dass auch danach eine unberechtigte Verarbeitung von personenbezogenen Daten verboten ist.

## 4.7 Rechte des Betroffenen

Die Rechte der Betroffenen zu stärken ist eines der besonderen Ziele der DS-GVO. Laut dieser darf niemand daran gehindert werden, seine Rechte auszuüben. Diese Rechte, welche zum Schutz des Betroffenen sind, können nicht durch Vertragsbedingungen oder Kollektivvereinbarungen ausgeschlossen werden. Für die EU-Mitgliedsstaaten gelten die gleichen Gesetze.

Art. 12 Transparente Information, Kommunikation	Art. 13. Informationspflicht bei Erhebung von Personenbezogenen Daten bei der betroffenen Person	Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
Art. 15 Auskunftsrecht der betroffenen Person	Art. 16 Recht auf Berichtigung	Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“)
Art. 18 Recht auf Einschränkung der Verarbeitung	Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder der Einschränkung der Verarbeitung	Art. 20 Recht auf Datenübertragbarkeit
Art. 21 Widerspruchsrecht	Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling	

## 4.8 Transparente Information und Kommunikation (Art.12 DS-GVO)

Die betroffene Person hat das Recht alle Informationen und Mitteilungen in präziser, transparenter, verständlicher und leicht zugänglicher Form übermittelt zu bekommen. Dies kann in schriftlicher, elektronischer oder auf Wunsch mündlicher Form stattfinden. Sollte die betroffene Person ihre personenbezogenen Daten anfordern, so muss die Zustellung an den Betroffenen innerhalb eines Monats erfolgen.

## Art. 12 Transparente Information, Kommunikation

1. Präzise, transparente, verständliche und leicht zugängliche Form in einer klaren und einfachen Sprache	2. Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte	3. Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag ergriffenen Maßnahmen unverzüglich (innerhalb eines Monats) zur Verfügung	4. Wird der Verantwortliche auf den Antrag des Betroffenen nicht tätig, so unterrichtet er den Betroffenen ohne Verzögerung (spätestens innerhalb eines Monats über die Gründe und die Möglichkeit Beschwerde bei der Aufsichtsbehörde einzulegen)	5. Informationen sowie alle Mitteilungen werden unentgeltlich zur Verfügung gestellt	6. Bei Zweifel des Verantwortlichen an der Identität der natürlichen Person, kann er unbeschadet zusätzliche Informationen anfordern	7. Kommunikation gegebenenfalls auch über Bilder (z.B. Bildsymbole)
---	---	--	--	--	--	---

### 4.9 Hat der Betroffene das Recht auf Informationen (aktive Informationen)?

Die DS-GVO regelt unter anderem auch die Informationspflichten des Verantwortlichen gegenüber dem Betroffenen. Sollte der Betroffene nun Gebrauch von seinem Recht auf Information machen, so ist der Verantwortliche dazu verpflichtet, diesen aktiv darüber zu unterrichten, sofern die betroffene Person die Informationen noch nicht vorliegen hat. Die Information muss folgendes enthalten:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Verarbeitungszweck der personenbezogenen Daten
- Rechtsgrundlage der Verarbeitung
- Sollte eine Interessenabwägung vorliegen, so müssen die berechtigten Interessen des Verantwortlichen enthalten sein
- Empfänger der Daten
- Ggf. Nachweise über Sicherheit beim Empfänger der Daten
- Voraussichtliche Speicherdauer
- Hinweis auf das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und Datenübertragbarkeit
- Sollte die Einwilligung die Rechtsgrundlage sein, so muss ein Hinweis erteilt werden, dass diese widerrufen werden kann
- Hinweis auf das Beschwerderecht bei der zuständigen Aufsichtsbehörde
- Auskunft darüber, ob Bereitstellung der personenbezogener Daten
  - gesetzlich,



- vertraglich vorgeschrieben oder
- für einen Vertragsabschluss erforderlich ist
- Bei automatisierter Entscheidungsfindung, die dahinter stehende Logik und die möglichen Auswirkungen auf die betroffene Person klären.
- Sollte sich der Zweck der Verarbeitung ändern, so muss vor der Weiterverarbeitung der neue Zweck der betroffenen Person mitgeteilt werden.
- Sollte der Betroffene die personenbezogenen Daten nicht angefordert haben, so ist der Verantwortliche dazu verpflichtet dem Betroffenen folgende Informationen zu melden:
  - Alle Informationen, die bei der Erhebung bei der betroffenen Person erforderlich sind
  - Aus welcher Quelle die Informationen stammen

Sollte es sich um Daten der Kommunikation mit der betroffenen Person handeln, erfolgt die Information spätestens zum Zeitpunkt der ersten Mitteilung. Zum Zeitpunkt der ersten Offenlegung erfolgt die Information dann, wenn die Offenlegung an einen anderen Empfänger gerichtet ist.

<h2 style="text-align: center; margin: 0;">Art 13. Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person</h2>			
<p>1. Zum Zeitpunkt der Erhebung wird dem Betroffenen von dem Verantwortlichen folgendes Mitgeteilt:</p> <p style="margin-left: 20px;">Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, die Zwecke, für die Verarbeitung der personenbezogenen Daten , wenn Verarbeitung auf Art.6 beruht die berechnete Interesse, gegebenenfalls die Empfänger der personenbezogenen Daten und gegebenenfalls die Absicht des Verantwortlichen die personenbezogenen Daten an Dritte weiter zu geben</p>	<p>2. Zum Zeitpunkt der Erhebung der Daten stellt der Verantwortliche dem Betroffenen folgende weitere Informationen zur Verfügung:</p> <p style="margin-left: 20px;">die Dauer wie lange personenbezogene Daten gespeichert werden, das Bestehen eines Rechts auf Auskunft, wenn Verarbeitung auf Art. 6 beruht, dass Recht die Einwilligung jederzeit zu widerrufen, das Bestehen eines Beschwerderechts, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist und das Bestehen einer automatisierten Entscheidungsfindung</p>	<p>3. Beabsichtigt der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiter zu verarbeiten, so stellt er dem Betroffenen vor der Weiterverarbeitung Informationen über diesen Zweck</p>	<p>4. Abschnitt 1,2 und 3 finden keine Anwendung, wenn und soweit der Betroffene bereits über die Informationen verfügt</p>

## Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

<p>1. Wenn personenbezogene Daten nicht bei dem Betroffenen erhoben werden so teilt der Verantwortliche folgendes mit: Namen und Kontaktdaten des Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke für die Verarbeitung, die Kategorien der personenbezogenen Daten, gegebenenfalls die Empfänger der Daten und gegebenenfalls die Absicht des Verantwortlichen die Daten an Dritte weiter zu geben</p>	<p>2. Zusätzlich stellt der Verantwortliche dem Betroffenen folgende Informationen: die Dauer der Verarbeitung, wenn die Verarbeitung auf Art. 6 beruht die berechtigten Interesse, das Bestehen eines Rechts auf Auskunft, das Recht die Einwilligung jederzeit zu widerrufen , das Bestehen eines Beschwerderechts, aus welcher Quelle die Daten stammen und das Bestehen einer automatisierten Entscheidungsfindung</p>	<p>3. Der Verantwortliche erteilt die Informationen gemäß 1. &amp; 2. : unter Berücksichtigung der spezifischen Umstände der Verarbeitung, falls die Daten zu Kommunikation mit dem Betroffenen verwendet werden und falls die Offenlegung an einen Empfänger beabsichtigt ist</p>	<p>4. Beabsichtigt der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiter zu verarbeiten, so stellt er dem Betroffenen vor der Weiterverarbeitung Informationen</p>	<p>5. 1. Bis 4. finden keine Anwendung, wenn: der Betroffene bereits über die Information verfügt, die Erteilung dieser Information sich als unmöglich erweist und die Erlangung oder Offenlegung durch Rechtsvorschriften der Union unterliegen und daher vertraulich behandelt werden müssen</p>
---	--	--	---	--

### 4.10 Hat der Betroffene ein Recht auf Auskunft (reaktive Information)?

Der Betroffene hat das Recht Auskunft darüber zu verlangen,

- Welche Daten von diesem erfasst wurden, zu welchem Zweck, woher diese stammen und wohin sie übermittelt werden.
- Für welchen Zeitraum diese Daten voraussichtlich verarbeitet werden.
- Auskunft muss innerhalb eines Monats erfolgen

## Art. 15 Auskunftsrecht der betroffenen Person

<p>1. Der Betroffene hat das Recht zu erfahren, ob seine personenbezogenen Daten verarbeitet werden. So hat er das Recht auf Auskunft und auf folgende Daten: Verarbeitungszweck, Kategorien der personenbezogenen Daten, die Empfänger der Daten, das Bestehen eines Rechts auf Berichtigung oder Löschung, das Bestehen eines Beschwerderechts, alle verfügbaren Daten über die Herkunft der personenbezogenen Daten und das Bestehen einer automatisierten Entscheidungsfindung</p>	<p>2. Sollten personenbezogene Daten an ein Drittland übermittelt werden, so hat der Betroffene das Recht darüber unterrichtet zu werden</p>	<p>3. Der Verantwortliche stellt eine Kopie der personenbezogenen Daten zur Verfügung</p>	<p>4. Das Recht auf Erhalt einer Kopie darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen</p>
--	--	---	--

#### 4.11 Hat man das Recht auf Berichtigung?

Sollten die personenbezogenen Daten des Betroffenen fehlerhaft sein, so hat dieser das Recht seine Daten vom Verantwortlichen und auch möglichen anderen Datenempfängern korrigieren zu lassen.

## Art. 16 Recht auf Berichtigung

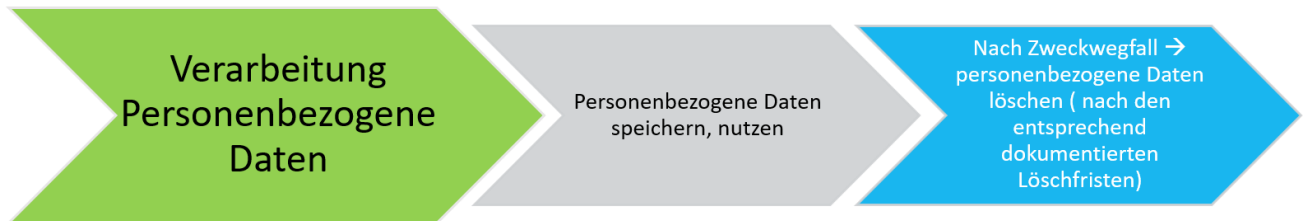
Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

#### 4.12 Hat der Betroffene das Recht auf Löschung seiner Daten? (Art. 17 DS-GVO)

Die betroffene Person hat das Recht darauf, den Verantwortlichen und mögliche Datenempfängern mitzuteilen, seine personenbezogenen Daten löschen zu lassen, sofern die weitere Verarbeitung der Daten nicht erforderlich ist. Sollte der Verantwortliche allerdings eine Aufbewahrungspflicht haben, so kann dies ein Hindernisgrund sein, die Daten löschen zu können. Im Steuerrecht findet sich beispielsweise dieses Aufbewahrungsrecht. Dort ist unter anderem festgelegt, dass Belege 10 Jahre aufgehoben werden müssen, bevor diese vernichtet werden können. Das Recht auf Löschung bezieht sich auch auf die Aufbewahrung von personenbezogenen Daten. Eine weitere Verarbeitung der personenbezogenen Daten ist unzulässig, wenn die Zweckbindung oder die Rechtsgrundlage der Verarbeitung wegfällt. Sollte diese wegfallen, so müssen die Daten gelöscht (zumindest anonymisiert) werden. Die personenbezogenen Daten müssen endgültig gelöscht, bzw. anonymisiert werden, wenn die Aufbewahrungsfrist abgelaufen ist.

# Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“)

<p>1. Der Betroffene hat das Recht, von dem Verantwortlichen zu verlangen, dass seine personenbezogenen Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:</p> <p>Die personenbezogenen Daten sind für ihre Zwecke nicht mehr notwendig</p> <p>Die betroffene Person widerruft ihre Einwilligung, auf die sich ihre Verarbeitung stützt</p> <p>Die betroffene Person legt gemäß Art. 21 Widerspruch gegen die Verarbeitung ein</p> <p>Die personenbezogenen Daten wurden unrechtmäßig verarbeitet</p> <p>Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung</p> <p>Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben</p>	<p>2. Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie angemessene Maßnahmen um für die Datenverarbeitung verantwortliche darüber zu informieren, dass eine betroffene Person von ihnen die Löschung ihrer Daten verlangt</p>	<p>3. Abschnitt 1. &amp; 2. gelten nicht, wenn die Verarbeitung erforderlich ist:</p> <p>Zur Ausübung des Rechts auf freie Meinungsäußerung und Information</p> <p>Zur Erfüllung einer rechtlichen Verpflichtung</p> <p>Aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit</p> <p>Für im öffentlichen Interesse liegenden Archivzweck</p> <p>Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen</p>
--	--	--



## 4.13 Hat man das Recht auf Einschränkung? (Art. 18 DS-GVO)

Der Betroffene hat die Möglichkeit seine Daten einschränken zu lassen, wenn das Löschen der Daten nur schwer möglich ist oder eine weitere Speicherung der Daten erforderlich ist. Um sie von zukünftigen Verarbeitungen ausschließen zu können, werden die betroffenen Daten markiert. Dieses Recht ist nur anwendbar, wenn die weitere Verarbeitung nicht erforderlich ist.

# Art. 18 Recht auf Einschränkung der Verarbeitung

<p>1. Der Betroffene hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:</p> <p>Die Richtigkeit der personenbezogenen Daten von dem Betroffenen bestritten wird</p> <p>Die Verarbeitung unrechtmäßig ist, jedoch die Löschung abgelehnt wird</p> <p>Der Verantwortliche die Daten für die Verarbeitung nicht länger benötigt, der Betroffene diese aber zu Ausübung oder Verteidigung von Rechtsansprüchen benötigt</p> <p>Der Betroffene Widerspruch gegen die Verarbeitung einlegt, jedoch solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen überwiegen</p>	<p>2. Wurde gemäß Abschnitt 1. eingeschränkt, so dürfen diese personenbezogenen Daten nur mit Einwilligung des Betroffenen oder zur Geltendmachung oder Ausübung von Rechtsansprüchen verarbeitet werden</p>	<p>3. Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Abschnitt 1. erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird</p>
---	--	---

## 4.14 Hat man das Recht auf eine Mitteilung im Zusammenhang mit der Berichtigung oder der Einschränkung der Verarbeitung? (Art. 19)

Der Betroffene hat das Recht von dem Verantwortlichen zu verlangen über die Verarbeitung seiner personenbezogenen Daten Auskunft zu erhalten, im Zusammenhang mit der Berichtigung oder der Einschränkung der Verarbeitung. Sollte der Verantwortliche also personenbezogene Daten Berichtigen oder Löschen, so muss er die betroffenen Person darüber in Kenntnis setzen. Jedoch muss er dies nicht tun, wenn dies mit einem unverhältnismäßig hohem Aufwand verbunden ist oder es sich als unmöglich erweist. Der Verantwortliche muss außerdem über diese Informationen Auskunft erteilen, wenn die betroffenen Person dies verlangt.

## Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder der Einschränkung der Verarbeitung

Der Verantwortliche teilt allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Art. 16, es sei denn dies erweist sich als unmöglich oder ist mit einem unverhältnismäßig hohem Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt

### 4.15 Hat man das Recht auf Datenübertragbarkeit? (Art. 20 DS-GVO)

Die personenbezogenen Daten kann sich der Betroffene in einem strukturierten, gängigen und maschinenlesbaren Format (von der verantwortlichen Stelle / Firma) herausgeben lassen. Hierbei kann er alle personenbezogenen Daten, welche er dem Verantwortlichen genannt hat, ausgehändigt bekommen. Die betroffene Person darf die erhaltenen personenbezogenen Daten an einen anderen Verantwortlichen weitergeben und dabei nicht von dem vorherigen Verantwortlichen gehindert werden.

## Art. 20 Recht auf Datenübertragbarkeit

1. Der Betroffene hat das Recht, die ihn betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinell lesbaren Format zu erhalten. Der Betroffene hat das Recht diese Daten einem anderen Verantwortlichen, ohne Behinderung durch den vorherigen Verantwortlichen, zu übermitteln, sofern  
Sofern die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht  
Die Verarbeitung mithilfe automatisierter Verfahren erfolgt

2. Bei der Ausübung ihres Recht der Datenübertragbarkeit hat die betroffene Person das Recht , zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

3. Die Ausübung dieses Rechts lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurden.

4. Das Recht gemäß Abschnitt 1. darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen

## 4.16 Hat man das Recht auf Widerspruch? (Art. 21 DS-GVO)

Die betroffene Person kann Widerspruch einlegen, sollte diese nicht wollen, dass ihre personenbezogenen Daten weiter verarbeitet werden. Die personenbezogenen Daten werden im Anschluss von dem Verantwortlichen nicht weiter verarbeitet, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, welche die Interessen, Freiheiten und Rechte der betroffenen Person überwiegen. Sollte die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dienen, so kann der Verantwortliche die personenbezogenen Daten weiter verarbeiten. Durch das Widerspruchsrecht wird besonders wegen der Direktwerbung vorgegangen, die aufgrund des Widerspruchs zu unterlassen ist.

Art. 21 Widerspruchsrecht					
1. Der Betroffene hat das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung Widerspruch einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interesse, Freiheiten und Rechte des Betroffenen überwiegen.	2. Wenn personenbezogene Daten verarbeitet werden um Direktwerbung zu betreiben, so hat der Betroffene das Recht Widerspruch gegen die Verarbeitung der personenbezogenen Daten zur Direktwerbung einzulegen.	3. Wenn der Betroffene gegen die Verarbeitung zum Zweck der Direktwerbung widerspricht, so werden seine personenbezogenen Daten für diesen Zweck nicht mehr weiter verarbeitet	4. Der Betroffene muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihm ausdrücklich auf das in 1. und 2. genannte Recht hingewiesen werden. Dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen	5. Im Zusammenhang mit der Nutzung von Informationsgesellschaften kann der Betroffene mittels automatisierter Verfahren sein Widerspruchsrecht ausüben	6. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung si betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erfolgt, Widerspruch einzulegen, es sei denn die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

## 4.17 Hat man das Recht auf nicht ausschließlich automatisierte Entscheidungen?

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Die Gewährung eines online beantragten Kredits darf beispielsweise nicht allein aufgrund mathematischer Algorithmen durchgeführt werden.



## Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

<p>1. Die betroffene Person hat das recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.</p>	<p>2. Abschnitt 1. gilt nicht, wenn die Entscheidung</p> <p>a) Für den Abschluss oder die Erfüllung eines Vertrags zwischen betroffener Person und dem Verantwortlichen erforderlich ist</p> <p>b) Aufgrund der Rechtsvorschrift der Union oder der Mitgliedsstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person seitens des Verantwortlichen gehört.</p> <p>c) Mit ausdrücklicher Einwilligung des Betroffenen erfolgt.</p>	<p>3. In den nach Abschnitt 2. Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten zu wahren.</p>	<p>4. Entscheidungen nach Abschnitt 2. dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Art. 9 beruhen.</p>
--	--	--	--

### 4.18 Hat man das Recht auf Beschwerde bei einer Aufsichtsbehörde?

Wenn die betroffene Person die Auffassung hat, dass sie in ihrer Freiheit und in ihrem Recht durch den Verantwortlichen eingeschränkt oder beraubt wird, so kann sich diese bei einer zuständigen Aufsichtsbehörde melden. Mögliche Aufsichtsbehörden wären diejenigen in dem EU-Mitgliedsstaat, ihres Arbeitsplatzes oder des Ortes des mutmaßlichen Verstoßes.

### 4.19 Hat man das Recht einen Datenschutzbeauftragten zu konsultieren?

Der Datenschutzbeauftragte des Verantwortlichen kann von der betroffenen Person zu allem, was die Verarbeitung ihrer personenbezogenen Daten angeht, zurate gezogen werden. Außerdem kann der Betroffene dem Datenschutzbeauftragten Fragen, die im Zusammenhang mit der Wahrnehmung seiner Rechte stehen, gemäß der Verordnung, stellen.



## 5 Verarbeitung von Daten durch externe Dienstleister

### 5.1 Beauftragung anderer Unternehmen mit personenbezogenen Daten

Es gibt keine Regelung der DS-GVO die vorschreibt, dass alle personenbezogenen Daten innerhalb eines Unternehmens selbst verarbeitet werden müssen. Gesetzlich ist vorgesehen, dass ein Unternehmen ein anderes Unternehmen mit der Verarbeitung von personenbezogenen Daten beauftragen kann. In Art. 28 DS-GVO sind die entsprechende Regelungen zur sogenannten Auftragsverarbeitung zu finden. Hier ist geregelt, unter welchen Rahmenbedingungen ein Auftrag an ein anderes Unternehmen erteilt werden darf. Es muss beispielsweise ein schriftlicher oder elektronischer Vertrag der Europäischen Union geschlossen werden. Wie und in welcher Weise die beauftragte Datenverarbeitung weisungsgebunden durch den Auftragnehmer stattfinden darf, ist in diesem Vertrag festgelegt. Somit sind beide, der Verantwortliche und der Auftragsverarbeitende dazu verpflichtet, für die Datenverarbeitung und die Einhaltung der DS-GVO zu sorgen. Der Verantwortliche ist verpflichtet den Auftragnehmer so auszuwählen, dass der Schutz der personenbezogenen Daten ausreichend gewährleistet werden kann. Dem Auftragsverarbeitendem ist untersagt, Unterauftragsnehmer einzusetzen, ohne dass die vorherige schriftliche Genehmigung vorliegt.

### 5.2 Was genau muss bei der Auftragsdatenverarbeitung festgelegt werden?

Der Mindestinhalt ist in Art. 28 DS-GVO vorgegeben. Dies muss eine Vereinbarung zur Auftragsverarbeitung enthalten:

- Der Zeitraum und der Gegenstand der Verarbeitung
- In welcher Art und zu welchem Zweck verarbeitet werden darf
- Um welche Art der personenbezogenen Daten es sich handelt
- Kategorie der betroffenen Menschen
- Die Pflichten und Rechte der Verantwortlichen
- Regelungen zur Beendigung des Auftragsverhältnisses:
  - Daten müssen an Verantwortlichen zurück gegeben werden
  - Datenschutzkonforme Löschung der Daten
- Pflichten des Auftragsverarbeitenden:

- Übermittlung und Verarbeitung nur auf Basis dokumentierter Weisungen durch den Verantwortlichen zulässig
- Wenn Weisungen des Verantwortlichen gegen den Datenschutz verstoßen, gilt Informationspflicht
- Verpflichtung zur Vertraulichkeit
- Technische oder organisatorische Maßnahmen zum Schutz personenbezogener Daten
- Einhaltung der Regelungen beim Einsatz eines weiteren Auftragsverarbeitenden
- Aus der Auftragsverarbeitung muss hervorgehen, dass die Pflichten eingehalten werden können
- Mitwirkungspflicht bei Überprüfungen seitens des Verantwortlichen
- Wenn Betroffene ihre Rechte wahrnehmen, den Verantwortlichen unterstützen
- Bei Vorliegen von melde- und benachrichtigungspflichtigen Sicherheitsverstößen den Verantwortlichen unterstützen.

### 5.3 Dokumentation darf nicht vergessen werden

Sollte eine Übermittlung personenbezogener Daten in einem Auftragsvertragsvertrag vorhanden sein, so sollte alles genau dokumentiert werden. Sollte eine betroffene Person eine Löschung oder Korrektur ihrer Daten beanspruchen, so müssen alle Empfänger der Daten entsprechend informiert werden.

### 5.4 Geltung der Bestimmungen zur Auftragsverarbeitung, wenn Verarbeitung nicht im Vordergrund steht

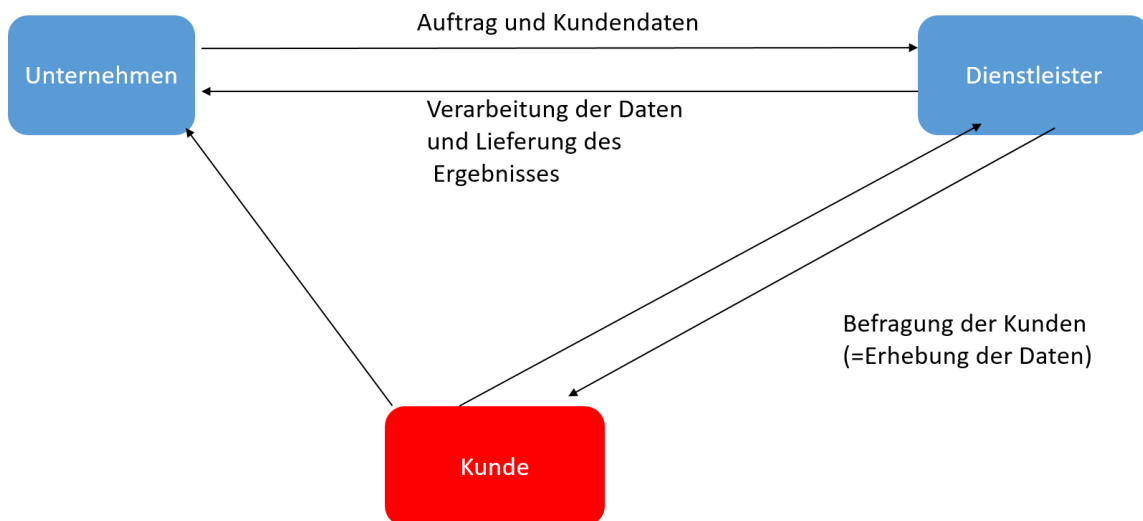
Selbst wenn die Verarbeitung personenbezogener Daten nicht im Vordergrund steht, gelten unter Umständen die Vorgaben zur Auftragsverarbeitung. Sollte ein Dienstleister beispielsweise bei Wartungs- oder Prüfungstätigkeit personenbezogene Daten einsehen, so fällt dies unter die Bereitstellung personenbezogener Daten und ist somit eine Verarbeitung, welche unter die Regelung der Auftragsverarbeitung fällt.

### 5.5 Wer ist zu informieren, wenn Tätigkeiten ausgelagert werden?

Sollten Tätigkeiten ausgelagert werden oder an andere Dienstleister vergeben werden, wobei personenbezogene Daten erhoben, verarbeitet

oder genutzt werden, sollte der betriebliche Datenschutzbeauftragte informiert werden. Von diesem kann geprüft werden, welche Maßnahmen aus datenschutzrechtlicher Sicht ergriffen werden müssen. Die Ergebnisse werden dem Unternehmen im Anschluss mitgeteilt.

Bsp.:



## 6 Datenaustausch innerhalb des Unternehmensverbundes

### 6.1 Was ist zu beachten, wenn Daten zwischen Unternehmen im Konzern oder Unternehmensverbund ausgetauscht werden sollen?

Sollte ein Unternehmen aus vielen rechtlich selbstständigen Unternehmen bestehen, so bedeutet diese Zusammengehörigkeit nicht, dass ohne weiteres von einem Unternehmen in ein anderes personenbezogene Daten übermittelt werden dürfen. Konzernprivilegien gelten für die DS-GVO nämlich nicht. Datenschutzrechtlich sind die Unternehmen innerhalb eines Konzerns so zu behandeln, als wären sie nicht miteinander verbunden, sondern völlig unabhängig von anderen Unternehmen.

### 6.2 Zu welchem Zeitpunkt dürfen Daten zwischen verbundenen Unternehmen ausgetauscht werden?

Auch hier gilt das Prinzip des Erlaubnisvorbehalts. Daten dürfen nicht an andere Konzerne weiter gegeben werden. Die DS-GVO sieht in Art. 6 Abs.1 lit. f als Erlaubnistatbestand das „berechtigte Interesse“ des Verantwortlichen. Als berechtigtes Interesse wird der Datenaustausch innerhalb einer Unternehmensgruppe zu Verwaltungszwecken als Erwägungsgrund gewertet. Als Erlaubnistatbestand muss die Einwilligung den Anforderungen des Art. 7 DS-GVO genügen.

## 7 Der Datenschutzbeauftragte (DSB)

### 7.1 Ab wann braucht ein Unternehmen einen Datenschutzbeauftragten?

Es werden prinzipiell Fälle vorgesehen, in denen ein Unternehmen, neben den öffentlichen Stellen, dazu verpflichtet ist, einen betrieblichen Datenschutzbeauftragten zu bestellen:

Der Datenschutzbeauftragte muss herangezogen werden, wenn die Haupttätigkeit des Verantwortlichen

- Es erforderlich macht, dass eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen durchgeführt werden muss.
- Darin besteht umfangreiche Verarbeitungen besonderer Kategorien von Daten oder Straftaten durchzuführen.
- Die EU-Mitgliedsstaaten gemäß Art. 37 Abs. 4 weitere Pflichten zur Bestellung festlegt.

Weitere Pflichten zur Bestellung sind in Deutschland gemäß Art 37 Abs. 4 der DS-GVO und §5 des BDSG neu festgelegt. Dies lässt sich in der DSAnpUG-EU finden, welches nationales, deutsches Recht an die Vorgaben der DS-GVO angepasst hat und somit die Öffnungsklausel der DS-GVO bedient:

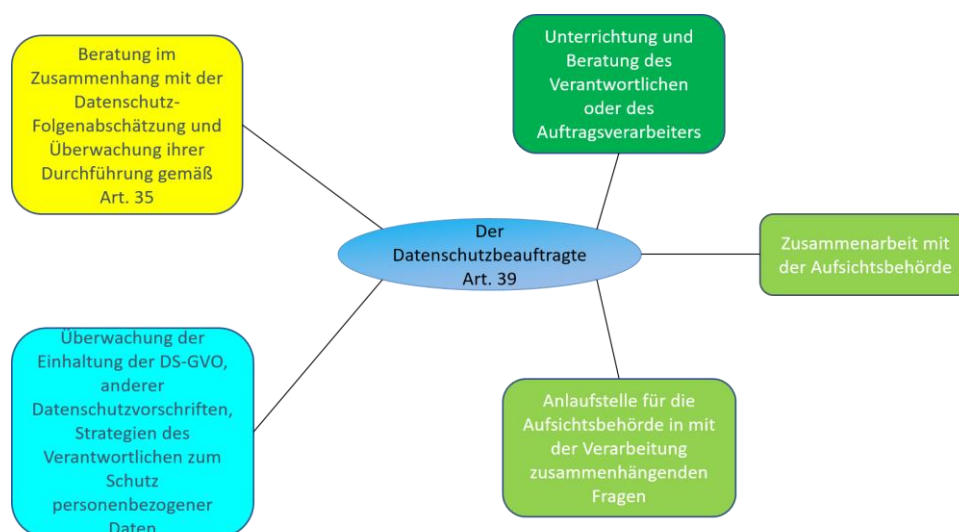
- Werden in einem Unternehmen in der Regel mehr als 9 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, dann muss das Unternehmen auch über einen betrieblichen Datenschutzbeauftragten verfügen (vgl. §38 Nr. 1 DSAnpUG-EU).  
Sollten allerdings nur bis zu 9 Personen sein, so braucht das Unternehmen zwar prinzipiell keinen Datenschutzbeauftragten. Allerdings muss die ursprüngliche Aufgabe des Datenschutzbeauftragten auf andere Weise sichergestellt werden.
- Sollen in einem Unternehmen Datenverarbeitungsverfahren zum Einsatz kommen, die wegen ihrer hohen Risiken für die betroffene Person eine Datenschutz-Folgeabschätzung gem. Art. 35 DS-GVO erforderlich machen, ist ebenfalls ein Datenschutzbeauftragter zu bestellen. Diese Regelung aus der DSAnpUG-EU §38, NR. 1) ergänzt ebenfalls die DS-GVO über eine Öffnungsklausel. Sofern der Verantwortliche einen Datenschutzbeauftragten benannt hat, sollte

dieser bei der Datenschutz-Folgeabschätzung, die vom Verantwortlichen durchzuführen ist, zu Rate gezogen werden; dies schreibt Art. 35 Nr. 2 DS-GVO vor.

- Auch wenn das Unternehmen personenbezogene Daten automatisiert verarbeitet, um dies an andere zu übermitteln, anonymisiert zu übermitteln oder diese zu Zwecken der Markt- und Meinungsforschung verarbeitet, ist ein Datenschutzbeauftragter erforderlich, ohne dass es auf die Anzahl der Mitarbeiter gem. §38, Nr. 1 DSAnpUG-EU ankommt.

## 7.2 Aufgaben des Datenschutzbeauftragten

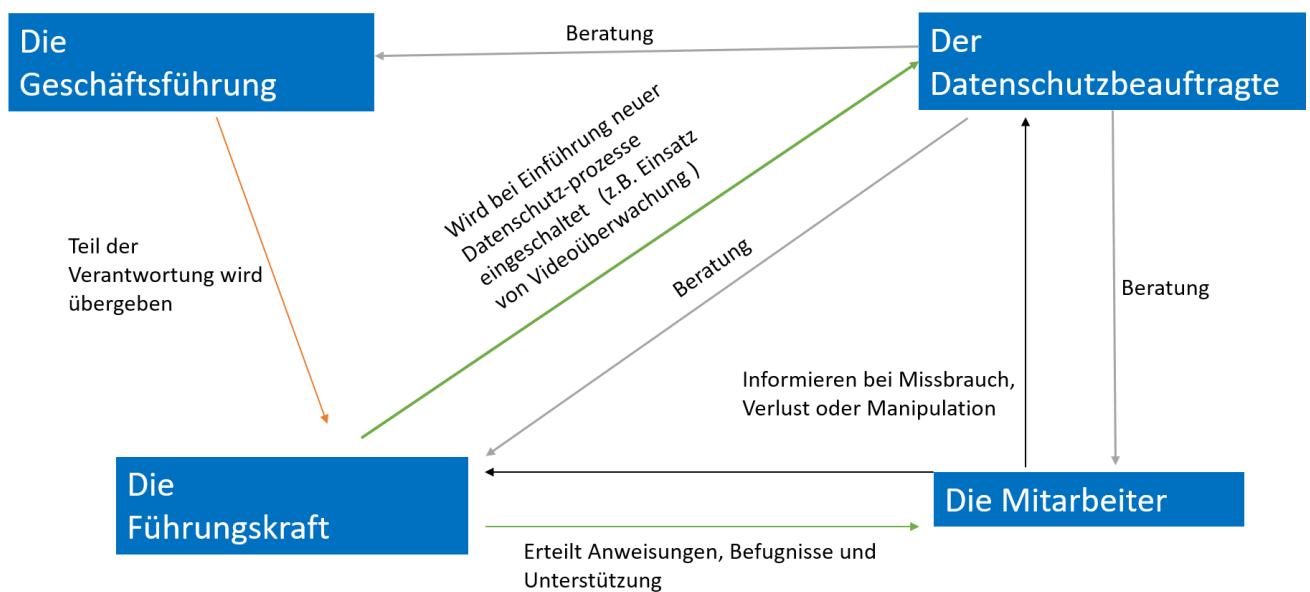
In Art. 39 DS-GVO hat der Gesetzgeber die wesentlichen Aufgaben eines Datenschutzbeauftragten (DSB) festgelegt. Der Datenschutzbeauftragte überwacht danach die Einhaltung der DS-GVO und andere Vorschriften über den Datenschutz (Art.39 Abs. 1 lit. b). Um den Schutz gewährleisten zu können, muss der Datenschutzbeauftragte darauf achten, dass die Datenverarbeitungsprozesse, in welchen personenbezogene Daten verarbeitet werden, ordnungsgemäß angewendet werden und somit nicht im Widerspruch zu den Vorgaben der DS-GVO stehen. Eine der zusätzlichen Aufgaben des Datenschutzbeauftragten ist es, Angestellte, welche in Kontakt mit personenbezogenen Daten kommen, mit den Datenschutzvorschriften vertraut zu machen. Sollten Mitarbeiter oder die Unternehmensleiter Fragen bezüglich der ordnungsgemäßen Verarbeitung personenbezogener Daten haben, so berät der Datenschutzbeauftragte hierbei. Der Datenschutzbeauftragte ist eine Anlaufstelle für die Aufsichtsbehörde und für betroffene Personen, welche Auskunft darüber erhalten möchten, wie mit den personenbezogenen Daten innerhalb des Unternehmens umgegangen wird. Er ist auch Ansprechpartner für Beschwerden im Umgang mit personenbezogenen Daten.



Die Geschäftsleitung (über die Bereichsleiter) entscheidet über die Prozesse / Abläufe. Der Datenschutzbeauftragte berät bei Fragen.

### 7.3 Sollte der Datenschutzbeauftragte bei neuen Datenverarbeitungsverfahren informiert werden?

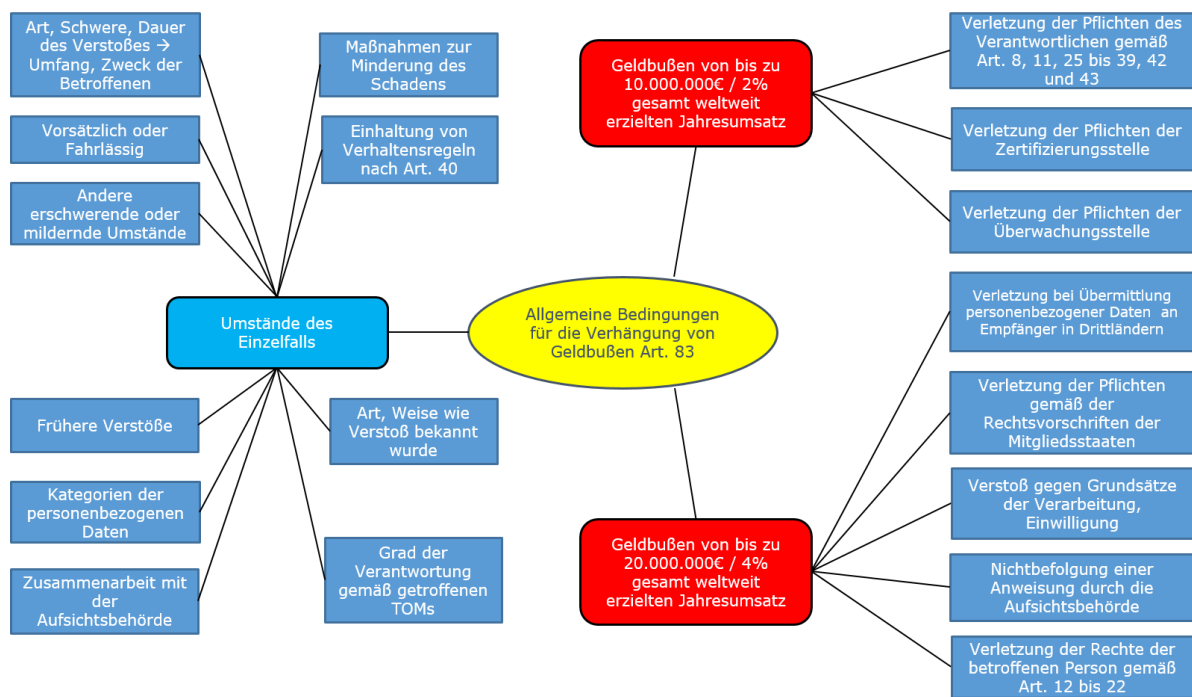
Damit die gesetzlichen Bestimmungen zum Datenschutz auch bei neuen Datenverarbeitungsverfahren ihre Richtigkeit aufweisen, sollte der Datenschutzbeauftragte ordnungsgemäß und frühzeitig informiert werden



# 8 Verstöße und Pannen des Datenschutzes

## 8.1 Welche Folgen hat ein Verstoß beim Datenschutz?

Sollte gegen die DS-GVO verstoßen werden, durch unrechtmäßiges Verarbeiten von personenbezogene Daten oder es werden organisatorische Anforderungen der DS-GVO nicht umgesetzt, kann dies Folgen für die Verantwortlichen und das Unternehmen haben. Die DS-GVO nennt solche Datenschutzpannen „Verletzung des Schutzes personenbezogener Daten“. Diverse Tatbestände sind in Art. 83 Abs. 4-6 aufgeführt, welche eine Geldbuße nach sich ziehen. Sollten beispielsweise auf einer Website keine datenschutzfreundlichen Angaben gemacht werden, so kann dies eine Geldstrafe von bis zu 10.000.000 € oder bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs nach sich ziehen, je nachdem welcher der Beträge der höhere ist (vgl. Art. 83 Abs. 4 lit. a). Sollten allerdings Verstöße gegen die Grundsätze des Datenschutzes getätigt werden, wie z.B. fehlende Einwilligungserklärungen oder Rechtsgrundlagen zur Verarbeitung, droht hierfür eine Geldstrafe von 20.000.000€ oder von bis zu 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist (vgl. Art. 83 Abs. 5 lit. a). Außerdem kann eine Datenschutzpanne den Ruf des Unternehmens nachhaltig beeinträchtigen. Es ist davon abhängig, wie schwerwiegend die Panne ist, z.B. kann es bei den Medien Jahre dauern, bis das Vertrauen wieder hergestellt ist.





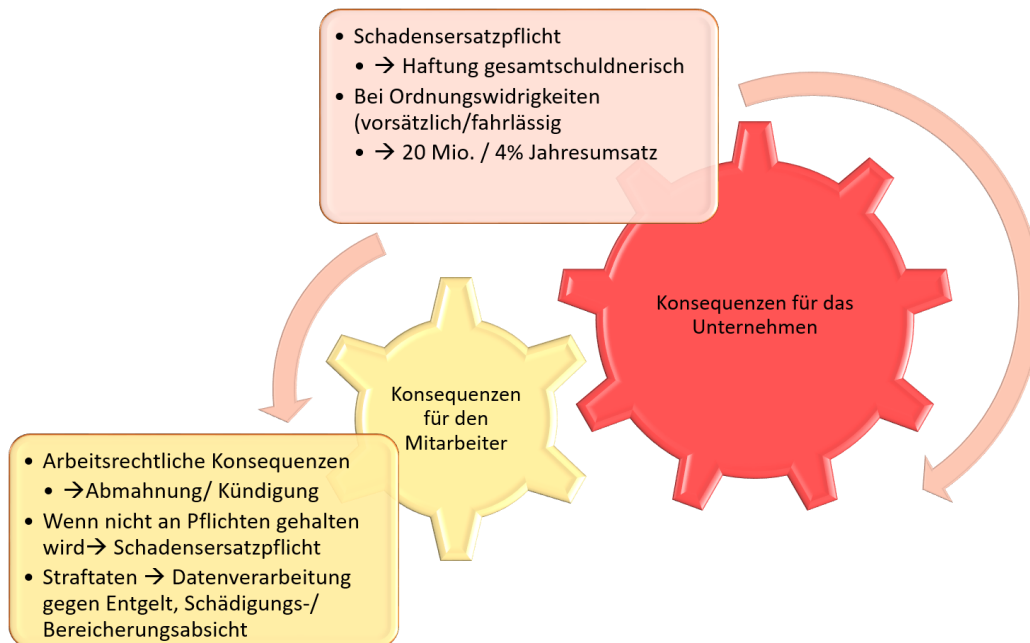
## 8.2 Wer muss informiert werden, wenn eine Verletzung des Datenschutzes entstanden ist?

Sollten Verletzungen des Datenschutzes in Bezug auf personenbezogene Daten entstehen, so muss dies unverzüglich mitgeteilt werden, binnen 72 Stunden. Dies ist in Art. 33 DS-GVO festgelegt. Nachdem die Verletzung bekannt geworden ist, muss die Aufsichtsbehörde informiert werden. Ausgenommen ist, wenn die Verletzung zu keinem Risiko für die Rechte und Freiheiten der betroffenen Person führt. Sollte jedoch ein Risiko für die betroffene Person entstehen, so muss diese ebenfalls darüber informiert werden. In Art. 33 und 34 DS-GVO wird aufgeführt welche Mindestanforderungen an den Inhalt, einer Meldung an die Aufsichtsbehörde und die betroffene Person, erfüllt werden müssen.



## 8.3 Kann eine Verletzung auch arbeitsrechtliche Konsequenzen haben?

Es kann zu arbeitsrechtlichen Konsequenzen führen, sollte es durch das Handeln eines Beschäftigten zu einem Datenschutzverstoß kommen. Sollte ein Schaden entstehen, welcher grob fahrlässig oder mit Absicht getätigt wurde, kann das Unternehmen vom Arbeitnehmer Schadenersatz verlangen. Darüber hinaus kann es zu einer arbeitsrechtlichen Abmahnung kommen, wenn eine Verletzung datenschutzrechtlicher Bestimmung erfolgt. Sollte es dem Unternehmen nicht möglich sein, den Arbeitnehmer weiter zu beschäftigen, kann eine Kündigung ausgesprochen werden. Bei schwerwiegenden Verstößen kann dies sogar fristlos erfolgen.



## 8.4 Schadensersatz für betroffene Personen

Betroffene Personen haben nach der DS-GVO Ansprüche auf Schadensersatz. Die betroffene Person hat dann ein Recht auf Schadensersatz, wenn sie durch den Verstoß gegen die DS-GVO einen materiellen oder immateriellen Schaden erleidet. Den Anspruch auf Schadensersatz hat die betroffene Person gegenüber dem Verantwortlichen oder dessen Auftragsverarbeitenden. Ebenfalls können Schadensersatzansprüche nach den Regeln des Bürgerlichen Gesetzbuches (BGB) bestehen, sollte durch die Verarbeitung personenbezogener Daten das grundgesetzlich geschützte Persönlichkeitsrecht eines Betroffenen beeinträchtigt werden.

## 8.5 Sollten dem Datenschutzbeauftragten Verstöße gemeldet werden?

Der Datenschutzbeauftragte sollte umgehend informiert werden, wenn einem Mitarbeiter ein massiver Verstoß gegen die DS-GVO auffällt, welcher durch einen anderen Mitarbeiter verursacht wurde. Dies hat nichts mit „Anschwärzen“ zutun. Eine solche Information trägt dazu bei, dass im Interesse aller Datenschutz und Datensicherheit gewährleistet bleiben und empfindliche Strafen vermieden werden.

Der DSB sollte auch informiert werden, wenn durch das Verhalten eines Mitarbeiters die Datensicherheit für personenbezogene Daten des Unternehmens bedroht ist. Sollte einem Mitarbeiter auffallen, dass besonders sensible oder personenbezogene Informationen gestohlen wurden oder dem Unternehmen auf andere Weise abhandengekommen

sind, muss unbedingt die Geschäftsleitung und der betriebliche Datenschutzbeauftragte informiert werden. Der Vorfall wird unter datenschutzrechtlichen Aspekten von dem Unternehmen und dem Datenschutzbeauftragten bewertet und das weitere Vorgehen wird festgelegt. Erforderlichenfalls ist die Aufsichtsbehörde für Datenschutz und die betroffene Person von der Geschäftsleitung zu informieren.



## 9 Unternehmen mit Videoüberwachung

### 9.1 Welche Regelungen müssen bei der Videoüberwachung eingehalten werden?

In der DS-GVO gibt es keine expliziten Regelungen zur Rechtsgrundlage von Videoüberwachung. Jedoch gibt es einige Hinweise auf deren Zulässigkeit. Daher ist die Videoüberwachung genauso wie alle Verarbeitungen mit personenbezogenen Daten zu handhaben. Eine Datenschutz-Folgen-Abschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche ist laut der Erwägungsgrundlage 91 Satz 3 erforderlich. Die Durchführung der Datenschutz-Folgeabschätzung wird in Art. 35 DS-GVO geregelt. Insbesondere ist diese nach Art. 35 Abs. 3 lit. c für die systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche erforderlich.

### 9.2 Gibt es Vorschriften außerhalb der DS-GVO zur Videoüberwachung?

Ein Unternehmen kann grundsätzlich aufgrund anderer rechtlicher Bestimmungen den Einsatz von Videokameras erlaubt bekommen oder dies kann sogar vorgeschrieben sein. Arbeitgeber und Mitarbeitervertretung können auch Vereinbarungen für die zulässige Videoüberwachung treffen. Kollektivvereinbarungen (einschließlich Betriebsvereinbarungen) als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im beschäftigten Kontext sind ein Beispiel.

### 9.3 Unterschied zwischen öffentlich zugänglichen und nicht öffentlich zugänglichen Räumen

Ein öffentlich zugänglicher Raum ist ein Raum oder eine Fläche, welche dazu bestimmt ist von jedermann betreten zu werden. Nicht öffentlich zugängliche Räume oder Flächen dürfen nur von einer bestimmten Personengruppe betreten werden. Dazu gehören innerhalb eines Unternehmens die Bereiche, in denen sich ausschließlich die Beschäftigten des Unternehmens aufhalten.

## 9.4 Gibt es einen Unterschied ob Bilddaten gespeichert werden oder nicht?

Auch das Beobachten von Bilddaten ohne eine Aufzeichnung, ist an den rechtlichen Zulässigkeitsvoraussetzungen zu messen. Die Bestimmungen der DS-GVO sind also auch einzuhalten, wenn eine Videokamera nur als „verlängertes Auge“ eingesetzt wird, z.B. wenn das Kamerabild einer Werkseinfahrt zum Monitor des Pförtners übertragen wird.

## 9.5 Darf heimlich videoüberwacht werden?

Die DS-GVO sieht keine Hinweispflicht für die Videoüberwachung vor und trifft auch keine Aussage zu einem heimlichen Einsatz von Videoüberwachung.

## 9.6 Dürfen bestimmte Bereiche nicht videoüberwacht werden?

Sollte die Videoüberwachung die Privat- und Intimsphäre der beobachteten Person unzumutbar beeinträchtigen, so ist die Überwachung in diesem Bereich Tabu. Solche Tabu-Bereiche wären beispielsweise Toiletten, Umkleiden, Waschräume, Gebetsräume, usw..

## 9.7 Wer prüft die Zulässigkeit einer Videoüberwachung?

Es ist die grundsätzliche Sache eines Unternehmens die Rechtsvorschriften der DS-GVO zur Videoüberwachung einzuhalten. Der betriebliche Datenschutzbeauftragte kann im Rahmen seiner Aufgaben bei der Datenschutz-Folgenabschätzung beratend tätig sein und eine Videoüberwachung datenschutzrechtlich bewerten. Dies ist auch im Rahmen seiner Überwachungsaufgabe möglich. Wichtige Prüfungspunkte dabei sind:

- Für welchen rechtlich zulässigen Zweck wird die Videoüberwachung eingesetzt?
- Welche Bereiche werden überwacht?
- Für welchen Zeitraum werden Bilddateien gespeichert und wann werden diese wieder gelöscht?
- Ist der Einsatz von Videoüberwachung auf das erforderliche Maß und insgesamt verhältnismäßig?

Die Zulässigkeit einer Videoüberwachungsmaßnahme kann auch die für das Unternehmen zuständige Aufsichtsbehörde für den Datenschutz überprüfen.

## 10 Datenverarbeitung im Beschäftigungsverhältnis

### 10.1 Welche Regelungen gibt es für den Umgang mit Beschäftigtendaten im Unternehmen?

„Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext [...] vorsehen“, heißt in Art. 88 DS-GVO.

Auch Vereinbarungen zwischen Unternehmen und Mitarbeitervertretung können verbindliche Regeln für das Verarbeiten personenbezogener Daten der Beschäftigten enthalten. Diese dürfen jedoch die zugeschriebenen Rechte der betroffenen Personen nicht aufheben.

### 10.2 Beschäftigte eines Unternehmens

Welche Personen in einem Unternehmen als beschäftigt gelten ist in § 26 Nr. 8 DSAnpUG-EU festgelegt. Dies sind insbesondere:

- Arbeitnehmerinnen und Arbeitnehmer,
- Auszubildende,
- Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis,
- Arbeitnehmerähnliche Personen, Heimarbeiter und Gleichgestellte sowie
- Personen, deren Beschäftigungsverhältnis beendet ist.

Für die Einordnung als Beschäftigter kommt es nicht auf die folgenden Aspekte:

- Verdienst
- Voll- oder Teilzeittätigkeit
- Haupt- oder nebenberufliche Tätigkeit
- Hierarchische Einordnung
- Wahrnehmung von Führungsaufgaben und Leitungsfunktionen

### 10.3 Wann darf ein Unternehmen personenbezogene Daten seiner Beschäftigten verarbeiten?

Sollten in einem Mitgliedstaat der Europäischen Union keine spezifischen Regelungen gemäß Art 88 DS-GVO gelten, so richtet sich die Rechtmäßigkeit der Verarbeitung allein nach der DS-GVO. Sofern die Regelungen des § 26 DSAnpUG-EU der DS-GVO nicht widersprechen, gelten diese. Der Verarbeitungszweck personenbezogener Daten der Beschäftigten ist daher zulässig, wenn dies für die Entscheidung über die Begründung, die Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Dabei liegt der Schwerpunkt darauf herauszufinden, ob die Verarbeitung zur Erreichung eines bestimmten Zwecks erforderlich ist.

### 10.4 Dürfen personenbezogene Daten von einem Unternehmen verarbeitet werden um Straftaten aufzudecken?

Um eine Straftat aufzudecken darf ein Unternehmen unter bestimmten Umständen personenbezogene Daten verarbeiten. Dies ist in §1 DSAnpUG-EU festgelegt. Solche Ermittlungsmaßnahmen sind zulässig, wenn:

- tatsächliche Anhaltspunkte den Verdacht begründen, dass ein Beschäftigter im Beschäftigungsverhältnis eine Straftat begangen hat und
- das Erheben, Verarbeiten und Nutzen personenbezogener Daten für die Aufdeckung der Straftaten erforderlich sind und sich
- der Beschäftigte auf kein überwiegendes schutzwürdiges Interesse am Ausschluss der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten berufen kann.

### 10.5 Muss die Mitarbeitervertretung dem Verfahren zustimmen?

Heutzutage kommt die Verarbeitung von personenbezogenen Daten fast ausnahmslos über Computer, Programme oder andere elektronische Datenverarbeitungsverfahren zum Einsatz. Gibt es in einem Unternehmen beispielsweise einen Betriebsrat als Arbeitervvertretung, so darf dieser nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) mitbestimmen. Bei solchen Verfahren handelt es sich schließlich in der

Regel um technische Einrichtungen, mit denen das Unternehmen das Verhalten oder die Leistung der Arbeitnehmer überwachen könnte.



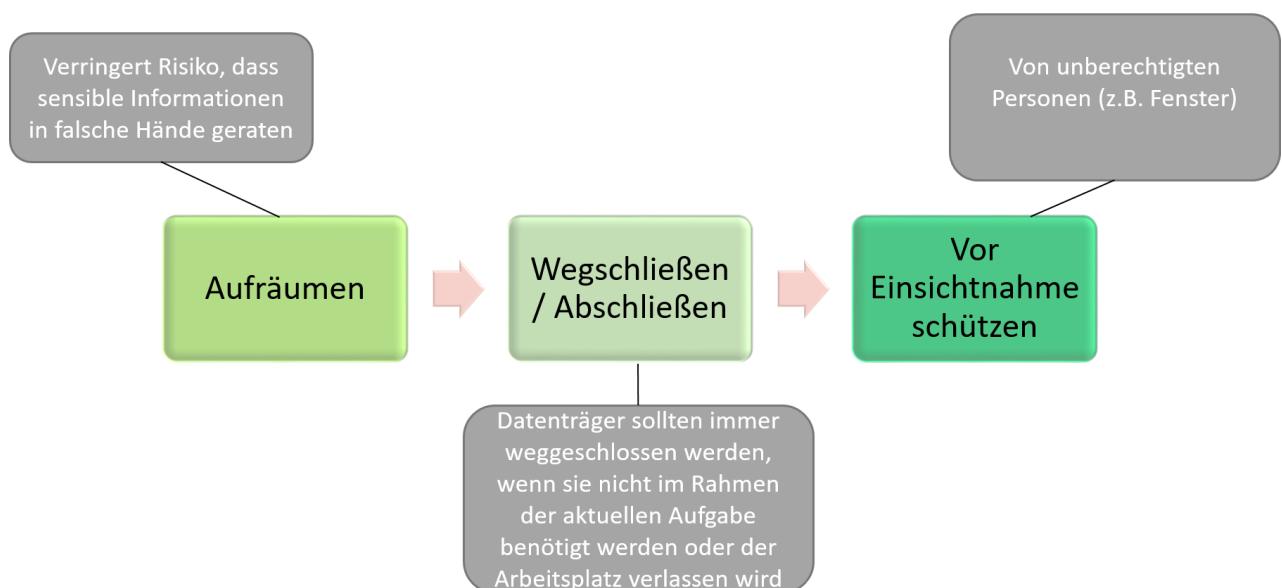
# 11 Datenschutz am Arbeitsplatz

## 11.1 Einhalten des Clean-Desk-Prinzips

Jeder kann dazu beitragen, dass personenbezogene Daten und vertrauliche Informationen geschützt werden. Besonders gut kann durch das sogenannte Clean-Desk-Prinzip für ausreichend Datenschutz am Arbeitsplatz gesorgt werden.

3 Regeln die hierbei besonders beherzigt werden sollten

- **Aufräumen**  
Ordnung hat nicht nur einen sehr praktischen Zweck, sondern kann auch das Risiko verringern, dass sensible Informationen in die falschen Hände gelangen.
- **Wegschließen**  
Datenträger, wie Notebooks, Smartphones, USB-Sticks oder Unterlagen sollten immer weggeschlossen werden, wenn sie nicht im Rahmen der aktuellen Arbeitsaufgabe genutzt werden.
- **Abschließen**  
Sollten sie beispielsweise zum Mittagessen gehen, also ihren Arbeitsplatz verlassen, so sollten Sie ihre Datenträger nicht nur in einem Behältnis verstauen, sondern abschließen. Wenn Sie den Schlüssel stecken lassen, bedarf es keines Spezialisten, um an den vertraulichen Inhalt zu kommen.



## 11.2 Sollte bei Passwörtern Mindestanforderungen beachtet werden?

Trivialpasswörter sollten sie bei der richtigen Auswahl eines Passwortes meiden. Unter einem sogenannten Trivialpasswort versteht man Passwörter, die einen Bezug zum Benutzer aufweisen, wie den Namen, Telefonnummer oder Geburtsdatum. Leicht zu erratende Passwörter oder Passwörter, welche in ihrer Schreibweise in Wörterbüchern oder Lexika zu finden sind, sollten ebenfalls gemieden werden. Um ein sicheres Passwort zu entwerfen, sollten die folgenden Passwortanforderungen berücksichtigt werden:

- Idealerweise besteht das Passwort aus **mindestens 10 Stellen**.
- Ziffern, Groß- und Kleinschreibung sowie Sonderzeichen sollten benutzt werden.
- Nebeneinanderliegende Tasten sollten gemieden werden.
- Das Passwort sollte nicht in Bezug gebracht werden mit dem Benutzer (ungeeignete Passwörter sind unter anderem also auch Kosenamen, Namen des Partners oder Lieblings Speisen).



## 11.3 Aufbewahrung von Passwörtern

Idealerweise sollten Passwörter **nur im eigenen Kopf** aufbewahrt werden, dabei ist jedoch klar, dass dies bei komplexen Passwörtern schwer fällt. Um sich Passwörter besser merken zu können, sollte man Eselsbrücken nutzen. Dies geht beispielsweise so: Sie bilden ihre Passwörter anhand der Anfangsbuchstaben leicht zu merkenden Sprüchen oder Liedzeilen. Aus der Liedzeile „99 Luftballons auf ihrem Weg zum Horizont, 99 Kriegsminister“ entsteht dieses Passwort: „99LBaiWzH, 99K“. Nach Möglichkeit sollten Sie ihr Passwort niemals aufschreiben, auch in Adressbüchern und Telefonlisten sollten diese nicht versteckt werden. Bei der Auswahl sicherer Speichermöglichkeiten hilft ihnen gerne ihre IT-Abteilung.

## 11.4 Sollten Passwörter Kollegen gegeben werden?

Passwörter gehen grundsätzlich nur Sie was an, dies betrifft auch den Kollegen, Vorgesetzten und Mitarbeiter der IT-Abteilung. Sollte sich nämlich jemand mit ihrem Passwort einloggen, so gibt sich dieser als Sie aus. Das kann schwerwiegende Folgen haben. Sollte ein Kollege mit den Zugangsdaten einen Schaden anrichten, so ist nur schwer zu beweisen, dass nicht Sie gehandelt haben. Daher sollten Sie schon aus Eigeninteresse Ihre Zugangsdaten nicht an Kollegen oder andere weitergeben. Außerdem sollten Sie Ihr Passwort unverzüglich ändern, wenn Sie den Verdacht haben, dass jemand Ihr Passwort mitbekommen hat.

## 11.5 Entsorgen von Unterlagen

Unterlagen mit personenbezogenen Daten dürfen nicht wie ganz normaler Hausmüll entsorgt werden, da nicht nur dem Unternehmen ein erheblicher Schaden droht, sollten diese in falsche Hände geraten können. Außerdem muss derjenige mit erheblichen Konsequenzen rechnen, der personenbezogene Daten leichtfertig entsorgt. Über den Papiermüll dürfen sensible Daten nur entfernt werden, wenn sichergestellt werden kann, dass Unbefugte an diese Daten nicht heran kommen. Damit sich Informationen von Papier nicht mehr zusammensetzen lassen, sollten Sie einen Aktenvernichter nutzen (siehe DIN 66399). Dokumente müssen Sie allerdings nicht in den Aktenvernichter geben, wenn ihnen eine spezielle Datenschutzone (sogenannte silberne Tonne) zur Verfügung steht.

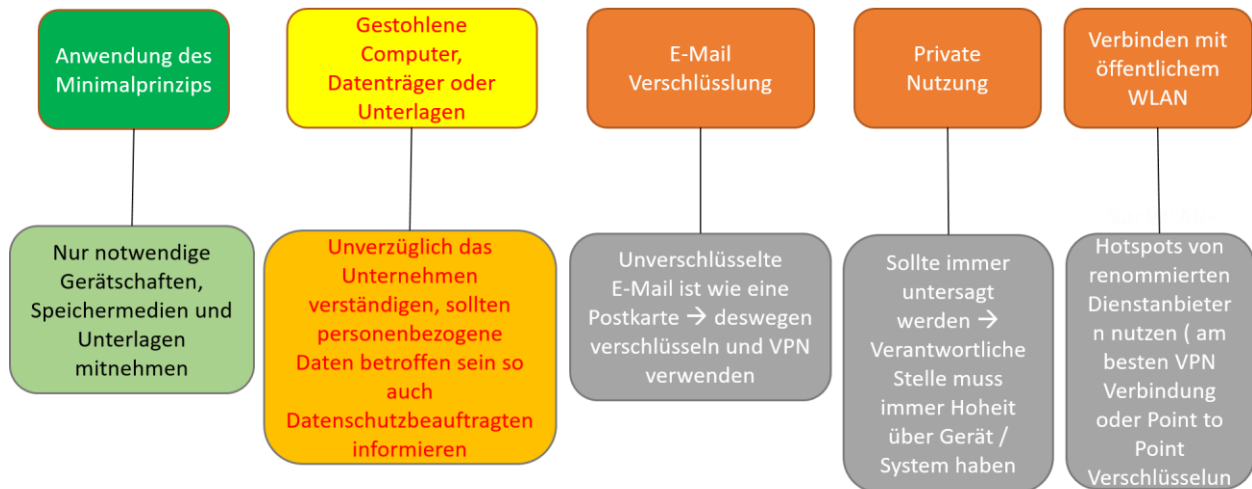
## 11.6 Was muss bei der Entsorgung von Datenträgern beachtet werden?

Sollten Datenträger entsorgt werden, so muss ebenso sichergestellt werden, dass gespeicherte personenbezogene Daten und vertrauliche Informationen nicht in falsche Hände geraten. Durch maschinelle Zerstörung des Datenträgers kann dies natürlich gewährleistet werden, aber auch durch datenschutzkonforme Löschung (siehe ebenso DIN 66399) ist es möglich, personenbezogene Daten zu entfernen. Jedoch reicht es nicht aus, wenn man dem Datenträger einen Formatierungsbefehl erteilt, da die Daten auf dem Datenträger erhalten bleiben. Es ist notwendig den Datenträger vollständig mit Nullen und Einsen zu überschreiben. Für geeignete Löschung von Daten können Sie ihre IT-Abteilung um Hilfe bitten.

## 11.7 Umgang mit Besuchern und Gästen

Auf dem Unternehmensgelände sollten sich Besucher nicht alleine bewegen dürfen. Sollten Sie also einen Kunden oder Gast erwarten, so sollten Sie diesen bei der Ankunft am Empfang abholen und bei der Abreise dort wieder hinbringen. So tragen Sie dazu bei, dass Unbefugte nicht auf Entdeckungsreise innerhalb des Unternehmens gehen.

## 12 Datenschutz unterwegs



### 12.1 Anwendung des Minimalprinzips

Sollten Sie auf Geschäftsreise sein brauchen Sie nicht ihre komplette Büroausstattung. Nehmen Sie deshalb nur diejenigen Gerätschaften, Speichermedien und Unterlagen mit, die Sie für ihre Arbeit unbedingt benötigen. Was Sie nicht dabei haben, kann weder gestohlen werden, noch abhandenkommen.

### 12.2 Aufbewahrung von Notebooks, Datenträgern und Unterlagen unterwegs

Diese sollten Sie immer so aufbewahren, dass sie den Blicken Unbefugter entzogen sind. Bei dem Transport im Auto sollten sie also nur im Kofferraum transportiert werden. Auch in Hotels sollten sie sicher verstaut werden, beispielsweise in einem Safe. Z.B. mittels eines Kabelschlosses sollte Ihr Notebook bei einer Tagung oder Besprechung gesichert werden. Dadurch brauchen Sie sich keine Sorgen machen, wenn Sie den Raum kurz verlassen und unter anderem machen Sie es potenziellen Dieben erheblich schwerer.

Zusätzlich sollten alle mobilen Geräte immer auch verschlüsselt werden (auch Speicherkarten, externe Festplatten usw.). Damit die Daten (beim Verlust des Gerätes) nicht von Unbefugten gelesen / verwendet werden können.

## 12.3 Verschlüsselung von Datenträgern und Daten

Sie machen es Unbefugten ziemlich schwer, wenn Sie ihren Datenträger oder ihre Daten verschlüsseln. Es gibt zahlreiche Verschlüsselungsmöglichkeiten, wie z.B. Anlegung eines verschlüsselten Datenarchivs (sogenannte ZIP-Datei). Sollte ein Datenträger also gestohlen werden, beschränkt sich der Schaden in erster Linie auf den materiellen Teil. Durch die Verschlüsselung der Daten ist der Zugriff erschwert und dadurch besteht in der Regel auch nur ein kleineres Risiko für Datenschutz und Vertraulichkeit.

## 12.4 E-Mail-Verschlüsselung

Eine E-Mail ist vergleichbar mit einer Postkarte, d.h. wenn sie nicht verschlüsselt ist, ist sie offen im Internet einsehbar. Aus diesem Grund sollten z.B. E-Mails in denen personenbezogene Daten vorhanden sind (Arbeitsverträge, Personalstammdaten) vom Personalbüro an den Steuerberater und umgekehrt immer nur verschlüsselt übertragen werden. Klären Sie mit Ihrer IT-Abteilung / Steuerberater welche Systeme Ihnen zur Verfügung gestellt werden können.

## 12.5 Besonders bedeutende Schutzmechanismen

Gerade wenn Sie unterwegs sind sollten Sie von vorhandenen Schutzmechanismen Gebrauch machen. Deaktivieren der Firewall oder Ausschalten der Überwachungsfunktion des Virenscanners sollten Sie unbedingt unterlassen. Gerade dann, wenn Sie mit ihrem Notebook ins Internet gehen, sind Firewall und Virenerkennung von großer Bedeutung. Personenbezogene Daten auf einem mobilen Datenträger sind immer besonders gegen unberechtigten Zugriff zu schützen. Sollten Sie keine drahtlose Verbindung benötigen, sollten Sie die entsprechenden Funktionen an Ihrem Notebook oder Smartphone abschalten.

## 12.6 Arbeit im Zug, Flugzeug und Hotellobby

Es kann vorkommen, dass Sie sich in einem sehr neugierigen Umfeld befinden, welches wissen möchte, was Sie gerade machen. Sie sollten nach Möglichkeit Ihren Sitzplatz so wählen, dass Ihnen nicht über die Schulter geschaut werden kann. Auch so genannte Sichtschutzfolien sind eine datenschutzfreundliche Hilfe. Diese sorgen dafür, dass eine andere Lichtbrechung zustande kommt und somit Ihr Sitznachbar nicht im Stande ist zu sehen, was auf Ihrem Bildschirm zu sehen ist.

## 12.7 Welches WLAN sollte für die Verbindung ins Internet genutzt werden?

Sollten Sie ihr Notebook mit dem WLAN verbinden wollen, sollten Sie immer WLAN-Hotspots nutzen, welche von renommierten Dienst Anbietern stammen. Bei anderen Dienst Anbietern oder sogenannten wilden WLAN-Hotspots können Sie sich nie sicher sein, welche Interessen der Anbieter tatsächlich verfolgt. Sie können alternativ natürlich auch Datenübertragungsdienste von Mobilfunk Anbietern nutzen. Eine Datenübertragung ist aber nur dann sicher, wie beim WLAN, wenn ihre Übertragung verschlüsselt ist.

## 12.8 Gestohlene Computer, Datenträger oder Unterlagen

Sollten Computer, andere Datenträger oder Dokumente gestohlen werden, muss unverzüglich das Unternehmen verständigt werden. Hierbei sollte der Vorgesetzte und die IT-Abteilung informiert werden. Sollten personenbezogene Daten oder vertrauliche Informationen betroffen sein, so muss der betriebliche Datenschutzbeauftragte ebenfalls hinzu gezogen werden. Die Stellen werden die Situation bewerten und geeignete Maßnahmen in die Wege leiten. Sollte Ihnen etwas gestohlen werden, sollten Sie ebenfalls Strafanzeige bei der örtlichen Polizei stellen und sich die Erstattung einer Anzeige bestätigen lassen.

## 12.9 Bring your own device (BYOD)

Unter diesem Begriff versteht man, dass Mitarbeiter ihr eigenes Equipment der Firma zur Verfügung stellen und innerhalb der Firma nutzen. Hiervon ist abzuraten. Hierfür ist ein erheblicher Aufwand der Dokumentation und Datensicherheit der Grund. Sollte es dennoch gewünscht werden, muss eine aufwendige Einzelfallprüfung stattfinden.

## 12.10 Homeoffice

Die verantwortliche Stelle (Firma) muss mit den Mitarbeitern alle vertraglichen Grundlagen so vereinbaren, dass zu jeder Zeit die Hoheit über die Daten bei der verantwortlichen Stelle liegt. D.h. Zugriff auf die jeweiligen Endgeräte, Sicherheitsanforderungen usw. müssen sauber dokumentiert und jeder Zeit überprüfbar sein. Hierbei ist im Allgemeinen ein höherer Arbeitsaufwand nötig.

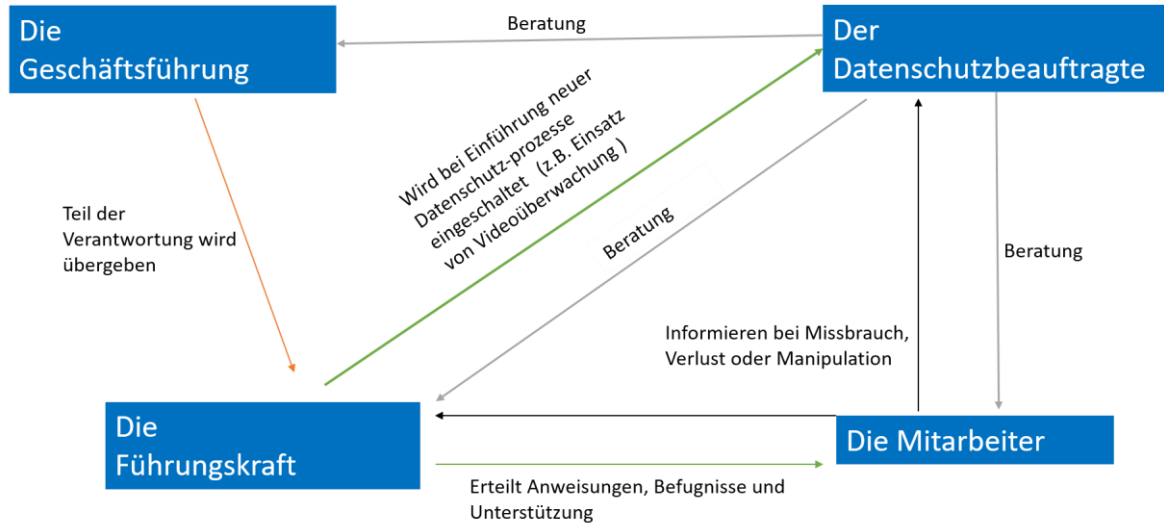
## 12.11 Private Nutzung

Private Nutzung von Firmenequipment sollte immer untersagt sein. Hintergrund ist, dass die verantwortliche Stelle immer die Hoheit über die Geräte/Systeme haben muss. Sollte es dennoch von der Geschäftsführung erwünscht sein, so sollte eine aufwendige Einzelprüfung der jeweiligen Anforderung durchgeführt werden.



# 13 Anlagen

## 13.1 Wer trägt in einem Unternehmen die Verantwortung



## 13.2 Rechte der betroffenen Person

Art. 12 Transparente Information, Kommunikation						
1. Präzise, transparente, verständliche und leicht zugängliche Form in einer klaren und einfachen Sprache	2. Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte	3. Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag ergriffenen Maßnahmen unverzüglich (innerhalb eines Monats) zur Verfügung	4. Wird der Verantwortliche auf den Antrag des Betroffenen nicht tätig, so unterrichtet er den Betroffenen ohne Verzögerung (spätestens innerhalb eines Monats) über die Gründe und die Möglichkeit Beschwerde bei der Aufsichtsbehörde einzulegen)	5. Informationen sowie alle Mitteilungen werden unentgeltlich zur Verfügung gestellt	6. Bei Zweifel des Verantwortlichen an der Identität der natürlichen Person, kann er unbeschadet zusätzlicher Informationen anfordern	7. Kommunikation gegebenenfalls auch über Bilder (z.B. Bildsymbole)

Art 13. Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person			
1. Zum Zeitpunkt der Erhebung wird dem Betroffenen von dem Verantwortlichen folgendes mitgeteilt: Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, die Zwecke, für die Verarbeitung der personenbezogenen Daten , wenn Verarbeitung auf Art.6 beruht die berechnete Interesse, gegebenenfalls die Empfänger der personenbezogenen Daten und gegebenenfalls die Absicht des Verantwortlichen die personenbezogenen Daten an Dritte weiter zu geben	2. Zum Zeitpunkt der Erhebung der Daten stellt der Verantwortliche dem Betroffenen folgende weitere Informationen zur Verfügung: die Dauer wie lange personenbezogene Daten gespeichert werden, das Bestehen eines Rechts auf Auskunft, wenn Verarbeitung auf Art. 6 beruht, dass Recht die Einwilligung jederzeit zu widerrufen, das Bestehen eines Beschwerderechts, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist und das Bestehen einer automatisierten Entscheidungsfindung	3. Beabsichtigt der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiter zu verarbeiten, so stellt er dem Betroffenen vor der Weiterverarbeitung Informationen über diesen Zweck	4. Abschnitt 1,2 und 3 finden keine Anwendung, wenn und soweit der Betroffene bereits über die Informationen verfügt

## Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

<p>1. Wenn personenbezogene Daten nicht bei dem Betroffenen erhoben werden so teilt der Verantwortliche folgendes mit: Namen und Kontaktdaten des Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke für die Verarbeitung, die Kategorien der personenbezogenen Daten, gegebenenfalls die Empfänger der Daten und gegebenenfalls die Absicht des Verantwortlichen die Daten an Dritte weiter zu geben</p>	<p>2. Zusätzlich stellt der Verantwortliche dem Betroffenen folgende Informationen: die Dauer der Verarbeitung, wenn die Verarbeitung auf Art. 6 beruht die berechtigten Interesse, das Bestehen eines Rechts auf Auskunft, das Recht die Einwilligung jederzeit zu widerrufen , das Bestehen eines Beschwerderechts, aus welcher Quelle die Daten stammen und das Bestehen einer automatisierten Entscheidungsfindung</p>	<p>3. Der Verantwortliche erteilt die Informationen gemäß 1. &amp; 2. : unter Berücksichtigung der spezifischen Umstände der Verarbeitung, falls die Daten zu Kommunikation mit dem Betroffenen verwendet werden und falls die Offenlegung an einen Empfänger beabsichtigt ist</p>	<p>4. Beabsichtigt der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiter zu verarbeiten, so stellt er dem Betroffenen vor der Weiterverarbeitung Informationen</p>	<p>5. 1. Bis 4. finden keine Anwendung, wenn: der Betroffene bereits über die Information verfügt, die Erteilung dieser Information sich als unmöglich erweist und die Erlangung oder Offenlegung durch Rechtsvorschriften der Union unterliegen und daher vertraulich behandelt werden müssen</p>
---	--	--	---	--

## Art. 15 Auskunftsrecht der betroffenen Person

<p>1. Der Betroffene hat das Recht zu erfahren, ob seine personenbezogenen Daten verarbeitet werden. So hat er das Recht auf Auskunft und auf folgende Daten: Verarbeitungszweck, Kategorien der personenbezogenen Daten, die Empfänger der Daten, das Bestehen eines Rechts auf Berichtigung oder Löschung, das Bestehen eines Beschwerderechts, alle verfügbaren Daten über die Herkunft der personenbezogenen Daten und das Bestehen einer automatisierten Entscheidungsfindung</p>	<p>2. Sollten personenbezogene Daten an ein Drittland übermittelt werden, so hat der Betroffene das Recht darüber unterrichtet zu werden</p>	<p>3. Der Verantwortliche stellt eine Kopie der personenbezogenen Daten zur Verfügung</p>	<p>4. Das Recht auf Erhalt einer Kopie darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen</p>
--	--	---	--

# Art. 16 Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

# Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“)

1. Der Betroffene hat das Recht, von dem Verantwortlichen zu verlangen, dass seine personenbezogenen Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für ihre Zwecke nicht mehr notwendig
- Die betroffene Person widerruft ihre Einwilligung, auf die sich ihre Verarbeitung stützt
- Die betroffene Person legt gemäß Art. 21 Widerspruch gegen die Verarbeitung ein
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben

2. Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie angemessene Maßnahmen um für die Datenverarbeitung verantwortliche darüber zu informieren, dass eine betroffene Person von ihnen die Löschung ihrer Daten verlangt

3. Abschnitt 1. & 2. gelten nicht, wenn die Verarbeitung erforderlich ist:

- Zur Ausübung des Rechts auf freie Meinungsäußerung und Information
- Zur Erfüllung einer rechtlichen Verpflichtung
- Aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
- Für im öffentlichen Interesse liegenden Archivzweck
- Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

## Art. 18 Recht auf Einschränkung der Verarbeitung

<p>1. Der Betroffene hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:</p> <p>Die Richtigkeit der personenbezogenen Daten von dem Betroffenen bestritten wird</p> <p>Die Verarbeitung unrechtmäßig ist, jedoch die Löschung abgelehnt wird</p> <p>Der Verantwortliche die Daten für die Verarbeitung nicht länger benötigt, der Betroffene diese aber zu Ausübung oder Verteidigung von Rechtsansprüchen benötigt</p> <p>Der Betroffene Widerspruch gegen die Verarbeitung einlegt, jedoch solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen überwiegen</p>	<p>2. Wurde gemäß Abschnitt 1. eingeschränkt, so dürfen diese personenbezogenen Daten nur mit Einwilligung des Betroffenen oder zur Geltendmachung oder Ausübung von Rechtsansprüchen verarbeitet werden</p>	<p>3. Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Abschnitt 1. erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird</p>
---	--	---

## Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder der Einschränkung der Verarbeitung

Der Verantwortliche teilt allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Art. 16, es sei denn dies erweist sich als unmöglich oder ist mit einem unverhältnismäßig hohem Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt

# Art. 20 Recht auf Datenübertragbarkeit

<p>1. Der Betroffene hat das Recht, die ihn betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinell lesbaren Format zu erhalten. Der Betroffene hat das Recht diese Daten einem anderen Verantwortlichen, ohne Behinderung durch den vorherigen Verantwortlichen, zu übermitteln, sofern</p> <p>Sofern die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht</p> <p>Die Verarbeitung mithilfe automatisierter Verfahren erfolgt</p>	<p>2. Bei der Ausübung ihres Recht der Datenübertragbarkeit hat die betroffene Person das Recht , zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.</p>	<p>3. Die Ausübung dieses Rechts lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurden.</p>	<p>4. Das Recht gemäß Abschnitt 1. darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen</p>
---	---	---	--

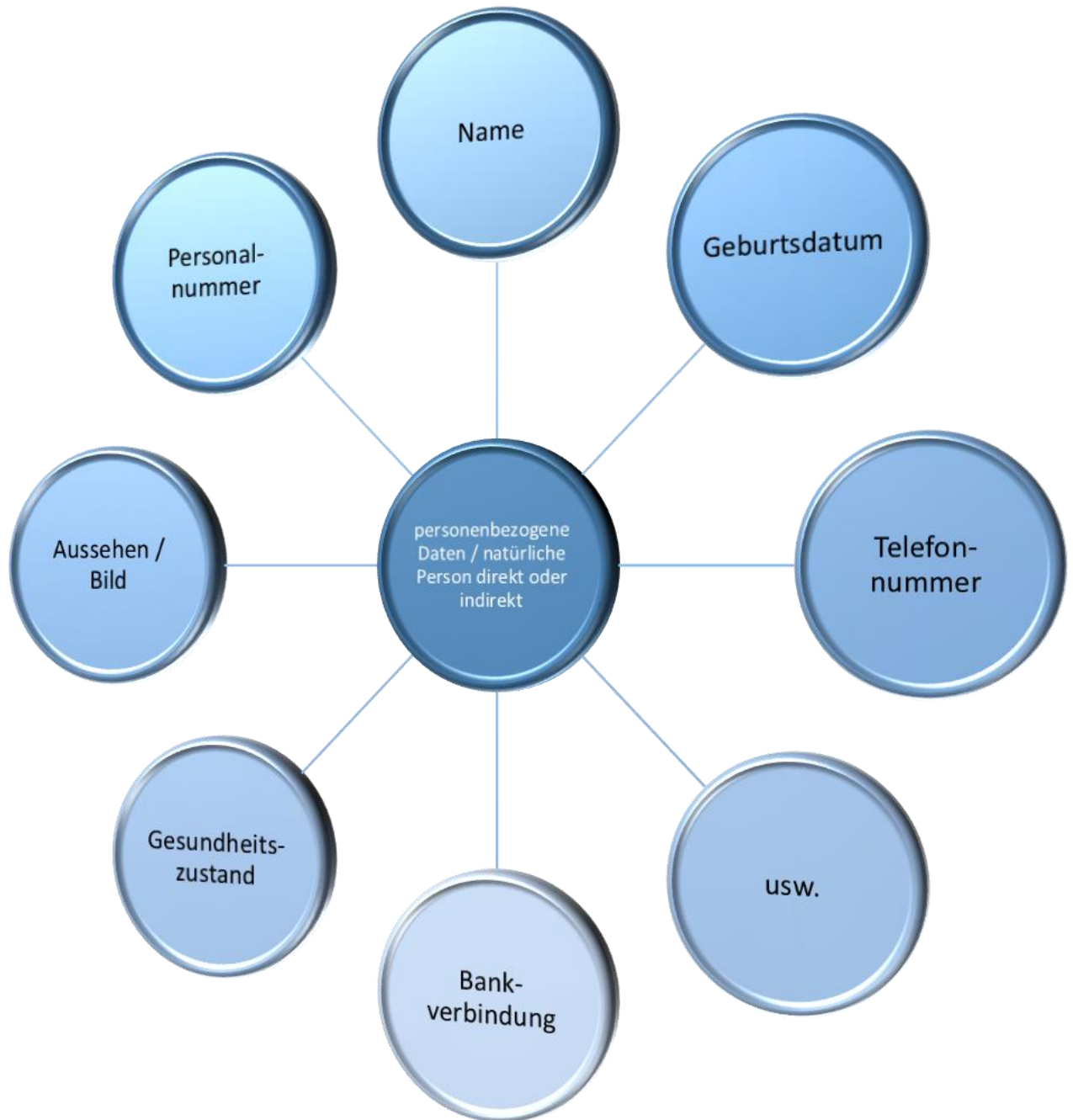
# Art. 21 Widerspruchsrecht

<p>1. Der Betroffene hat das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung Widerspruch einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interesse, Freiheiten und Rechte des Betroffenen überwiegen.</p>	<p>2. Wenn personenbezogene Daten verarbeitet werden um Direktwerbung zu betreiben, so hat der Betroffene das Recht Widerspruch gegen die Verarbeitung der personenbezogenen Daten zur Direktwerbung einzulegen.</p>	<p>3. Wenn der Betroffene gegen die Verarbeitung zum Zweck der Direktwerbung widerspricht, so werden seine personenbezogenen Daten für diesen Zweck nicht mehr weiter verarbeitet</p>	<p>4. Der Betroffene muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihm ausdrücklich auf das in 1. und 2. genannte Recht hingewiesen werden. Dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen</p>	<p>5. Im Zusammenhang mit der Nutzung von Informationsgesellschaften kann der Betroffene mittels automatisierter Verfahren sein Widerspruchsrecht ausüben</p>	<p>6. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung von personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erfolgt, Widerspruch einzulegen, es sei denn die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.</p>
---	--	---	---	---	--

# Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

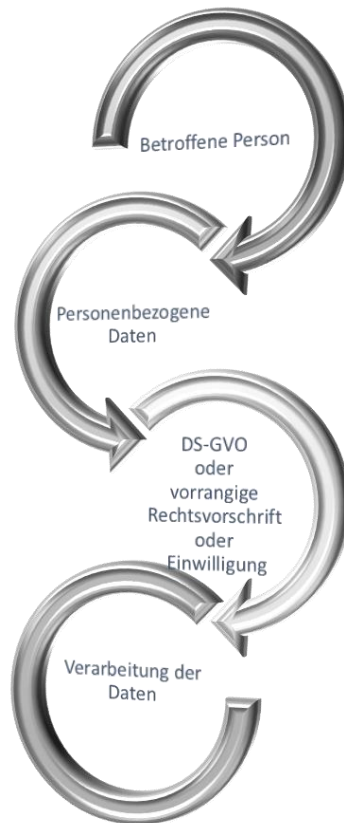
<p>1. Die betroffene Person hat das recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.</p>	<p>2. Abschnitt 1. gilt nicht, wenn die Entscheidung</p> <p>a) Für den Abschluss oder die Erfüllung eines Vertrags zwischen betroffener Person und dem Verantwortlichen erforderlich ist</p> <p>b) Aufgrund der Rechtsvorschrift der Union oder der Mitgliedsstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person seitens des Verantwortlichen gehört.</p> <p>c) Mit ausdrücklicher Einwilligung des Betroffenen erfolgt.</p>	<p>3. In den nach Abschnitt 2. Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten zu wahren.</p>	<p>4. Entscheidungen nach Abschnitt 2. dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Art. 9 beruhen.</p>
--	--	--	--

## 13.3 personenbezogene Daten

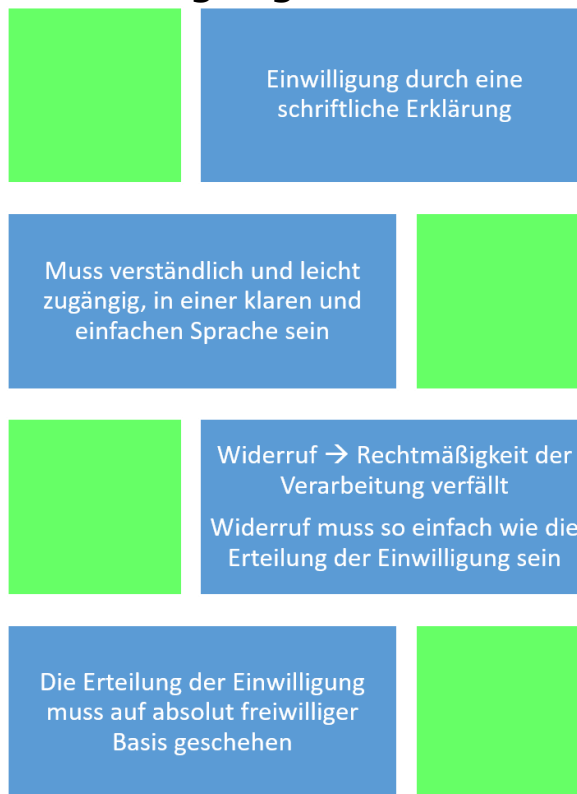




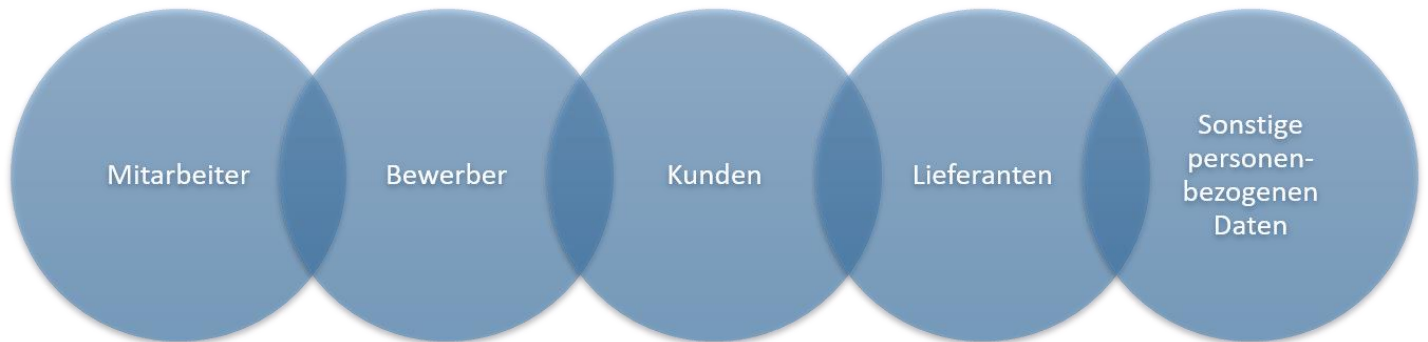
## 13.4 Richtigkeit der Verarbeitung



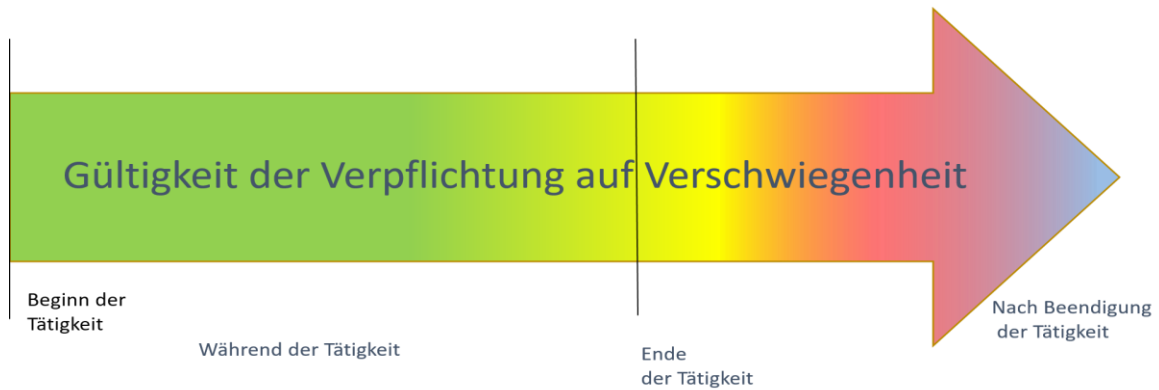
## 13.5 Die Einwilligung



## 13.6 Datenschutz im Unternehmen



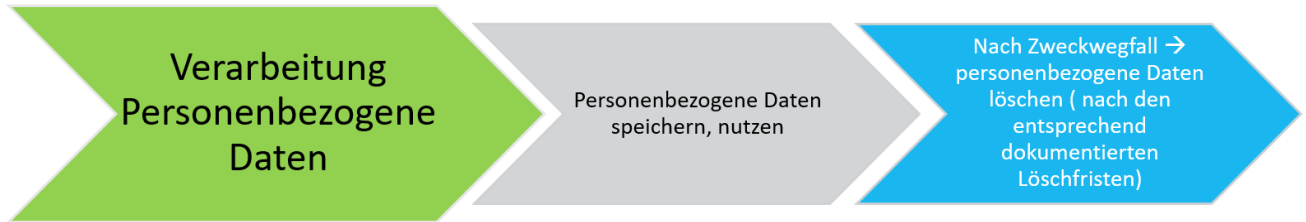
## 13.7 Gültigkeit der Verpflichtung auf Verschwiegenheit



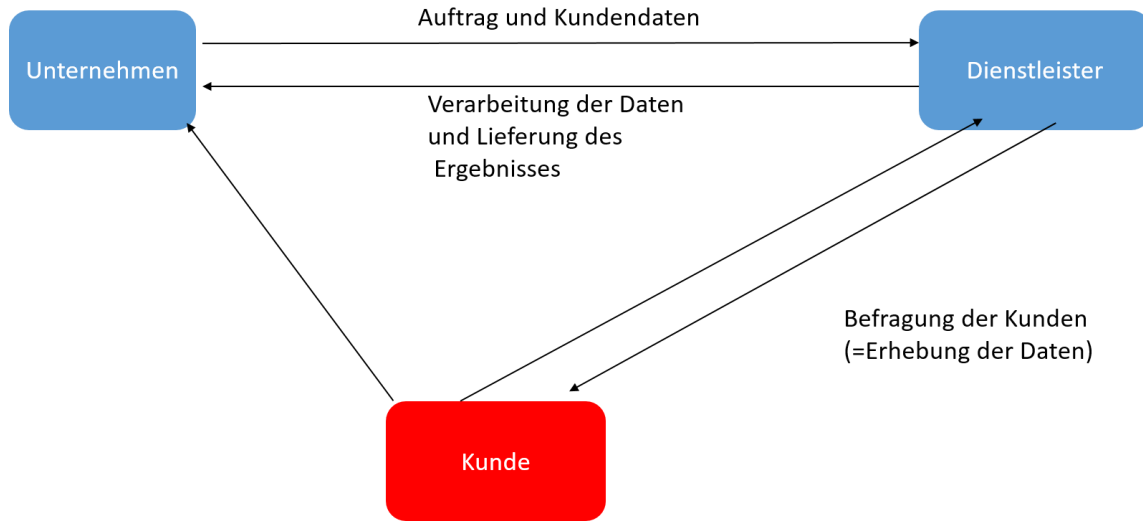
## 13.8 Rechte der betroffenen Person

Art. 12 Transparente Information, Kommunikation	Art. 13. Informationspflicht bei Erhebung von Personenbezogenen Daten bei der betroffenen Person	Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
Art. 15 Auskunftsrecht der betroffenen Person	Art. 16 Recht auf Berichtigung	Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“)
Art. 18 Recht auf Einschränkung der Verarbeitung	Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder der Einschränkung der Verarbeitung	Art. 20 Recht auf Datenübertragbarkeit
Art. 21 Widerspruchsrecht	Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling	

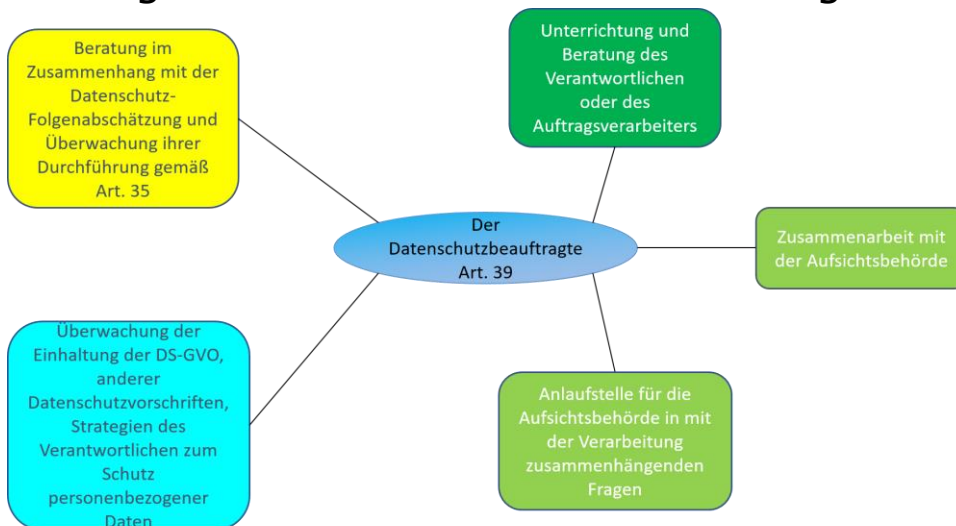
### 13.9 Schritte der Verarbeitung



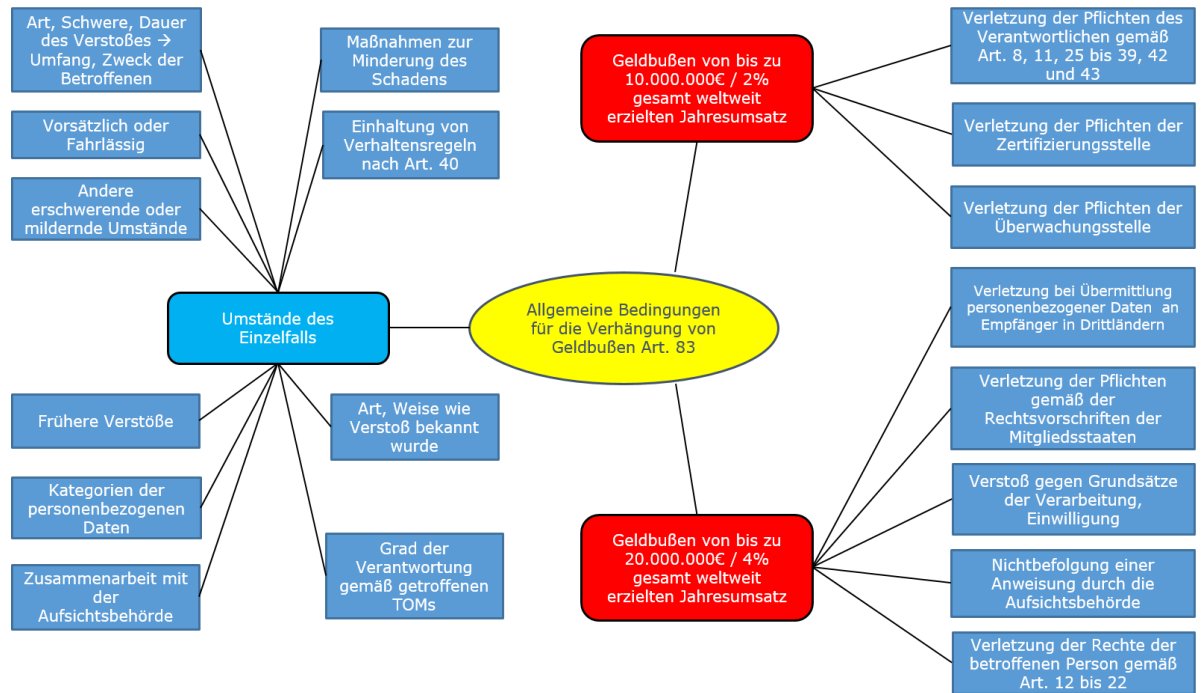
### 13.10 Datenfluss und Tätigkeiten bei der Auftragsdatenverarbeitung Bsp.



### 13.11 Aufgaben des Datenschutzbeauftragten



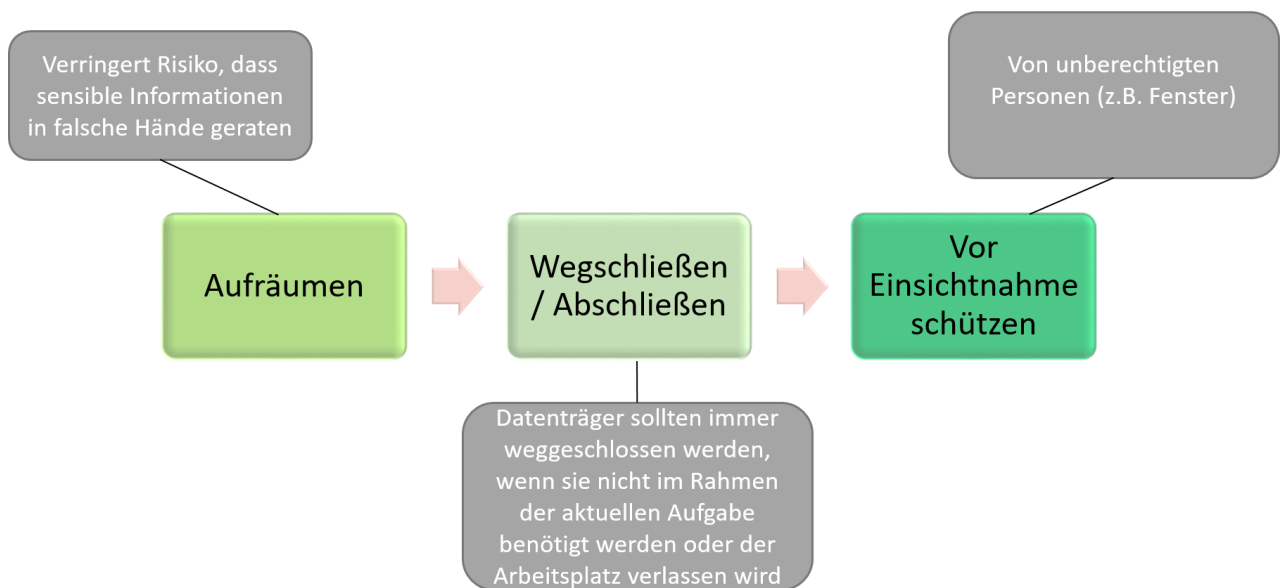
### 13.12 Allgemeine Bedingungen für die Verhängung von Geldbußen Art 83



### 13.13 Prozess beim Entdecken von Verstößen



### 13.14 Clean-Desk-Prinzip



### 13.15 Wer trägt die Konsequenzen?

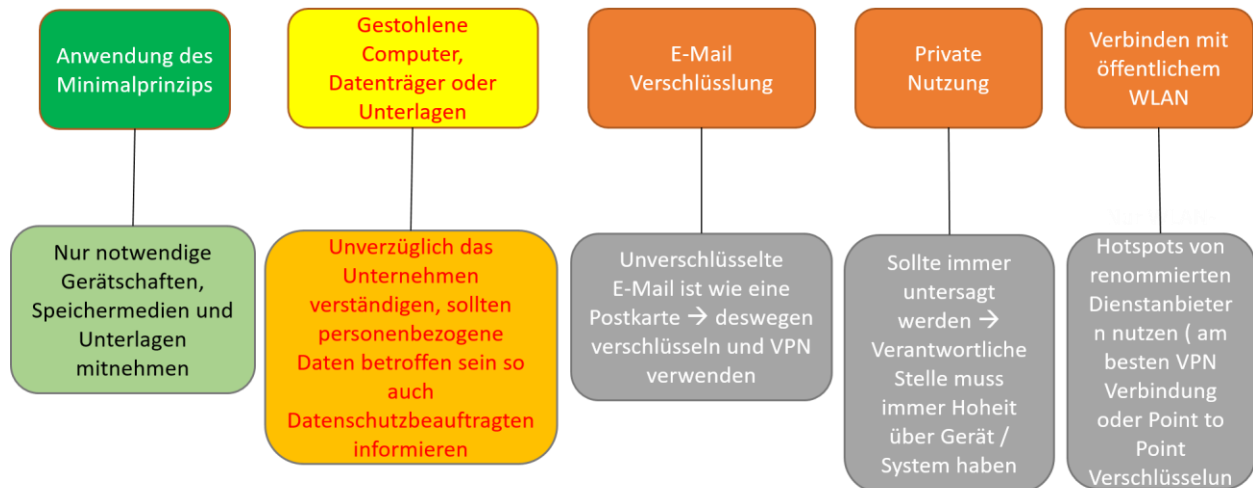


### 13.16 Mindestanforderungen bei der Passwortwahl

## Mindestanforderungen bei der Passwortwahl

Besteht aus mindestens 10 Stellen	Ziffern, Groß- und Kleinschreibung sowie Sonderzeichen	Nebeneinanderliegende Tasten vermeiden	Passwort darf nicht in Bezug mit dem Benutzer gebracht werden	Nur im eigenen Kopf behalten ( nicht aufschreiben, keinen Kollegen verraten)	Es darf kein aussprechbares Wort sein
-----------------------------------	--	--	---	--	---------------------------------------

## 13.17 Datenschutz unterwegs



# LovoSoft GmbH

Geschäftsstelle  
Auf der Beune 85  
64839 Münster (Hessen)  
+49(0) 163 2983007  
[info@lovosoft.de](mailto:info@lovosoft.de)