Wirtschaftsverband Stahl- und Metallverarbeitung e.V.

Unverbindlicher Datenschutz – Leitfaden

Einleitung

Der WSM Wirtschaftsverband Stahl- und Metallverarbeitung e.V. ist ein Dachverband verschiedener Industrieverbände der Stahl und Metall verarbeitenden Branchen in Deutschland. Die Mitgliedsunternehmen sind vorwiegend mittelständisch geprägte Industrieunternehmen.

Der WSM erkennt das Recht auf informationelle Selbstbestimmung, den notwendigen Schutz der Privatsphäre und die Sicherheit der Datenverarbeitung an. Die rechtsverbindlichen nationalen und europäischen Regelungen zum Datenschutz müssen eingehalten werden. Die Grundsätze einer fairen und transparenten Datenverarbeitung, der Erforderlichkeit der verarbeiteten Daten und der Datenvermeidung sowie der Datensparsamkeit sind zu beachten.

Der WSM empfiehlt seinen Mitgliedsunternehmen nachfolgende Regeln zum Umgang mit personenbezogenen Daten. Das Ziel dieser Leitlinien ist die Förderung der Einhaltung von datenschutzrechtlichen Regelungen durch die Beschreibung grundlegender Standards.

Die Regeln sind nicht verbindlich und allgemeingültig formuliert. Den Unternehmen bleibt es unbenommen, andere oder weitere Regelungen z.B. mit datenschutzrechtlichem Mehrwert zu treffen. Haben die Unternehmen bereits eigene Regelungen getroffen, bleiben diese unberührt.

Art. 1 Geltungsbereich / Personenbezogene Daten

1. Die Regeln gelten für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Unternehmen.

2. Gemäß Art. 4 Nr. 1 DSGVO sind personenbezogene Daten Angaben über eine identifizierte oder identifizierbare natürliche Person (z.B. eigene oder fremde Mitarbeiter, nicht jedoch juristische Personen, wie z.B. GmbH). Identifiziert ist eine Person, wenn sie z.B. konkret namentlich benannt ist. Identifizierbar ist eine Person, wenn die Möglichkeit besteht, ihre Identität z.B. über eine Telefonnummer zu ermitteln.

Personenbezogene Daten sind z.B.:

- Name, Adresse, Geburtsdatum
- Telefon-, Personal-, Kontonummer
- E-Mail-Adresse mit Namen (mustermann@gmbh.com)
- KfZ-Kennzeichen
- IP-Adresse

Keine personenbezogenen Daten sind z.B.:

- E-Mail-Adresse ohne Namen (info@gmbh.com)
- Produktionsdaten, technische Zeichnungen

3. Unbeschadet der hier getroffenen Regelungen gelten die Vorschriften des Bundesdatenschutzgesetzes (BDSG) und der Datenschutz-Grundverordnung (DSGVO).

Art. 2 Grundsatz und Zweckbestimmung

1. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erfolgt grundsätzlich nur, soweit dies zur Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses erforderlich ist. Sie erfolgt auch zur Erfüllung rechtlicher - d.h. gesetzlicher und vertraglicher - Verpflichtungen, zur Wahrung berechtigter Interessen und auf der Basis von Einwilligungen der Betroffenen.

2. Die personenbezogenen Daten werden grundsätzlich nur im Rahmen der den Betroffenen bekannten Zweckbestimmung erhoben, verarbeitet und genutzt. Eine Änderung oder Erweiterung der Zweckbestimmung erfolgt nur, wenn sie rechtlich zulässig ist und die Betroffenen darüber informiert wurden oder wenn die Betroffenen eingewilligt haben.

3. Die Zweckbestimmung ergibt sich aus dem Vertragsverhältnis selbst (z.B. Arbeitsvertrag), aus Gesetzen oder Verordnungen oder einer Datenschutzerklärung, die das Unternehmen dem Betroffenen übergibt oder im Internet veröffentlicht. Die Betroffenen erhalten Transparenz über den Umgang mit ihren personenbezogenen Daten.

Art. 3 Grundsätze zur Qualität der Datenerhebung, -verarbeitung und -nutzung

1. Die Unternehmen verpflichten sich, alle personenbezogenen Daten in fairer, rechtmäßiger und den schutzwürdigen Interessen der Betroffenen entsprechender Weise zu erheben, zu verarbeiten und zu nutzen.

2. Die Datenerhebung, -verarbeitung und -nutzung richtet sich an dem Ziel der Datenvermeidung und Datensparsamkeit aus (Art. 5 DSGVO). Dies kann eine Anonymisierung und Pseudonymisierung bedeuten, soweit dies möglich und der Aufwand nicht unverhältnismäßig zu dem angestrebten Schutzzweck ist.

3. Die verantwortliche Stelle beim Unternehmen trägt dafür Sorge, dass die vorhandenen personenbezogenen Daten richtig und auf dem aktuellen Stand gespeichert sind. Es werden angemessene Maßnahmen dafür getroffen, dass nicht zutreffende oder unvollständige Daten berichtigt, gelöscht oder gesperrt werden.

Art. 4 Grundsätze der Datensicherheit

Zur Gewährleistung der Datensicherheit werden die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO getroffen. Dabei sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit) und
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Art. 5 Datenschutz-Management-System

1. Die Unternehmen geben sich ein Datenschutz-Management-System, in dem die betrieblichen Prozesse zur Einhaltung und Umsetzung des Datenschutzes nachvollziehbar beschrieben werden. Das Datenschutz-Management-System wird unter Einbeziehung der betrieblichen Datenschutzbeauftragten erstellt, dokumentiert, regelmäßig geprüft und wenn erforderlich aktualisiert.

2. Das Datenschutz-Management-System umfasst regelmäßig

   - die Benennung von einem oder von mehreren betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO
   - ggf. die Benennung eines Konzern-Datenschutzbeauftragten gemäß Art. 37 Abs. 2 DSGVO
   - das Führen eines Verarbeitungsverzeichnisses gemäß Art. 30 DSGVO

Art. 6 Datenschutzsicherheitskonzept

1. Die in den Unternehmen veranlassten Maßnahmen werden in ein die Verantwortlichkeiten regelndes Datenschutzsicherheitskonzept integriert, welches unter Einbeziehung der betrieblichen Datenschutzbeauftragten erstellt, dokumentiert, regelmäßig geprüft und aktualisiert wird.

2. Die technischen Maßnahmen zum Schutz der Datensicherheit entsprechen jederzeit dem Stand der Technik.

3. Der Aufwand steht in einem angemessenen Verhältnis zu dem Erhebungszweck, den Risiken für den Betroffenen und der Art sowie dem Umfang der Daten. Kleinere und mittlere Unternehmen dürfen grundsätzlich einen geringeren Aufwand betreiben als große Unternehmen.

4. Das Unternehmen trifft geeignete technische Maßnahmen, um den unbefugten Zugriff auf personenbezogene Daten durch Personen aus der eigenen Organisation oder von außen abzuwehren.

5. Physisch verkörperte personenbezogene Daten z.B. in Papieren werden vor unbefugten Zugriffen Dritter geschützt, indem sie sorgfältig, ggf. verschlossen, verwahrt werden. Der Zugang zu Büroräumen ist zu kontrollieren. Sensible Bereiche (z.B. Personalbüro) erfahren einen höheren Schutz als andere Bereiche. Durch entsprechende technische Vorrichtungen und Anweisungen an die Mitarbeiter ist der Schutz sicher zu stellen. Das Unternehmen stellt sicher, dass personenbezogene Daten datenschutzkonform gelöscht bzw. vernichtet werden. Dies wird regelmäßig den Einsatz von Datenvernichtern, Datenschutztonnen oder Dienstleistern implizieren.

6. Zum Schutz digital erfasster personenbezogener Daten werden

    - PCs mit Passwortschutz versehen, wobei die Passwörter regelmäßig geändert werden,
    - Berechtigungskonzepte entwickelt.

Art. 7 Datenschutz-Folgenabschätzung

1. Soweit eine Form der Verarbeitung voraussichtlich ein Risiko für Recht und Freiheit natürlicher Personen zur Folge hat, kann vor Aufnahme der Verarbeitung eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO durchgeführt werden. Zur Beurteilung des Erfordernisses der Datenschutz-Folgeabschätzung werden die Risken der Betroffenen ermittelt, analysiert und der Höhe nach beurteilt.

2. Sind die Risiken als hoch einzustufen, ist die Datenschutz-Folgenabschätzung durchzuführen, insbesondere wenn zwei der folgenden Risikofaktoren zutreffen:

    - Systematische und umfassende Erfassung und Bewertung persönlicher Aspekte natürlicher Personen,
    - automatisierte Einzelentscheidung,
    - Scoring/Profiling,
    - Verarbeitung sensibler Daten,
    - großer Umfang der Datenverarbeitung,

- Zusammenführung von Daten,
- besonders gefährdete Personen (insb. Kinder)
- neue/innovative Technologien,
- internationaler Datentransfer,
- Verhinderung Rechteausübung Betroffener.

Art. 8 Einwilligung

1. Soweit die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten auf eine Einwilligung der Betroffenen gemäß Art. 7 DSGVO gestützt wird, stellt das Unternehmen sicher, dass diese auf der freien Entscheidung der Betroffenen beruht, wirksam und nicht widerrufen ist.

2. Soweit die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von Minderjährigen auf eine Einwilligung gestützt wird, werden diese Erklärungen von dem gesetzlichen Vertreter eingeholt. Mit der Vollendung des 18. Lebensjahres werden diese Erklärungen von diesem selbst eingeholt.

3. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Ist die Einwilligung zur Durchführung des Vertrages oder der Erfüllung einer rechtlichen Verpflichtung erforderlich, ist ein Widerruf ausgeschlossen oder führt dazu, dass die Leistung nicht erbracht werden kann. Das einholende Unternehmen stellt sicher, dass die Betroffenen zuvor über den Umfang, die Form und den Zweck der Datenerhebung, -verarbeitung oder -nutzung sowie die Möglichkeit der Verweigerung und die Widerruflichkeit der Einwilligung und deren Folgen informiert sind.

4. Grundsätzlich wird die Einwilligung in Schrift- oder Textform (z.B. E-Mail oder Fax) eingeholt. Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, wird sie räumlich getrennt und optisch hervorgehoben. Im Falle besonderer Umstände, z.B. in Eilsituationen oder wenn der Kommunikationswunsch von den Betroffenen ausgegangen ist, und wenn die Einholung einer Einwilligung auf diesem Wege im besonderen Interesse der Betroffenen liegt, kann die Einwilligung auch mündlich erteilt werden. Wird die Einwilligung mündlich eingeholt, ist dies zu dokumentieren und den Betroffenen mit der nächsten Mitteilung in Schrift- oder Textform, wenn dies dem Vertrag oder der Anfrage des Betroffenen entspricht, zu bestätigen.

5. Eine Einwilligung kann elektronisch erteilt werden, wenn der Erklärungsinhalt aktiv bestätigt wird.

6. Einwilligungen eigener Arbeitnehmer dürfen nur auf freiwilliger Basis eingeholt werden. Die Arbeitnehmer sind darauf hinzuweisen, dass eine Verweigerung der Einwilligung für sie keine nachteiligen Konsequenzen haben wird.

Art. 9 Datenverarbeitung innerhalb der Unternehmensgruppe

1. An Dritte werden personenbezogene Daten nach dem Grundsatz der Vertraulichkeit nur weitergegeben, wenn dies aufgrund einer rechtlichen Verpflichtung

erfolgt oder nach Maßgabe der folgenden Regeln.

2. Wenn das Unternehmen einer Gruppe von Unternehmen angehört, können personenbezogene Daten in einem von Mitgliedern der Gruppe gemeinsam nutzbaren Datenverarbeitungsverfahren erhoben, verarbeitet oder genutzt werden, wenn sichergestellt ist, dass die technischen und organisatorischen Maßnahmen den datenschutzrechtlichen Anforderungen entsprechen und die Einhaltung dieser Regeln gewährleistet ist. Das gilt auch für verbundene Einzelunternehmen oder Handelsvertreter.

3. Die Betroffenen werden darüber in geeigneter Form informiert, z.B. auf der Homepage des Unternehmens. Das Unternehmen hält eine aktuelle Liste aller Unternehmen der Gruppe bereit, die an einer zentralisierten Bearbeitung teilnehmen.

Art. 10 Funktionsübertragung an Auftragsdatenverarbeiter

1. Die Übermittlung von personenbezogenen Daten an Auftragsdatenverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO zur eigenverantwortlichen Erfüllung von Datenverarbeitungs- oder sonstigen Aufgaben kann erfolgen, wenn dies zur Wahrung der berechtigten Interessen des Unternehmens erforderlich ist und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse des Betroffenen dem entgegensteht.

2. Die Übermittlung von personenbezogenen Daten an Auftragsdatenverarbeiter unterbleibt, soweit der Betroffene dieser widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse des übermittelnden Unternehmens überwiegt.

3. Das Unternehmen schließt mit den Auftragsdatenverarbeitern, die in seinem Interesse tätig werden, eine vertragliche Vereinbarung gemäß Art. 28 Abs. 3 DSGVO, die mindestens folgende Punkte enthalten muss:

   - Beschreibung der Aufgaben des Dienstleisters;
   - Sicherstellung, dass die übermittelten Daten nur im Rahmen der vereinbarten Zweckbestimmung verarbeitet oder genutzt werden;
   - Gewährleistung eines Datenschutz- und Datensicherheitsstandards, der diesen Regeln entspricht;
   - Verpflichtung des Dienstleisters, dem Unternehmen alle Auskünfte zu erteilen, die zur Erfüllung einer beim Unternehmen verbleibenden Auskunftspflicht erforderlich sind oder dem Betroffenen direkt Auskunft zu erteilen und
   - Verpflichtung des Dienstleisters, bei Datenpannen unverzüglich die erforderlichen Maßnahmen zu ergreifen.

4. Das Unternehmen hält eine aktuelle Liste der Auftragsdatenverarbeiter bereit, an die Aufgaben im Wesentlichen übertragen werden. Ist die systematische

automatisierte Verarbeitung personenbezogener Daten nicht Hauptgegenstand des Vertrages, können die Dienstleister in Kategorien zusammengefasst werden unter Bezeichnung ihrer Aufgabe.

5. Das Unternehmen stellt sicher, dass die Rechte der Betroffenen durch die Einschaltung des Auftragsdatenverarbeiters nicht geschmälert werden.

Art. 11 Übermittlung personenbezogener Daten an Nicht-EU Länder

1. Die grenzüberschreitende Übermittlung von Daten an Empfänger in Drittländern kann vorgenommen werden, wenn die EU-Kommission gemäß Art. 45 Abs. 1 DSGVO festgestellt hat, dass das betreffende Drittland über ein angemessenes Schutzniveau verfügt. Derzeit handelt es sich um folgende Drittländer: Andorra, Argentinien, Färöer, Israel, Isle of Man, Kanada, Guernsey, Jersey, Schweiz und Uruguay – aktuelle Übersicht auf den Websites der Europäischen Kommission (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_de).

2. Die Unternehmen können personenbezogene Daten ohne Angemessenheitsbeschluss übermitteln, indem sie durch den Abschluss von EU-Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 c) DSGVO mit der empfangenden Stelle geeignete Garantien schaffen und ein angemessenes Datenschutzniveau sicherstellen. Den Unternehmen ist bewusst, dass diese EU-Standarddatenschutzklauseln nicht verändert werden dürfen.

3. Grenzüberschreitende Übermittlungen innerhalb von Unternehmen oder Unternehmensgruppen kann das Unternehmen durch interne Datenschutzvorschriften gemäß Art. 47 DSGVO rechtfertigen. Dem Unternehmen ist bewusst, dass diese internen Datenschutzvorschriften von der zuständigen Aufsichtsbehörde genehmigt werden müssen.

4. Verantwortliche Stellen oder Auftragsverarbeiter in Drittländern können bestimmte Verarbeitungsvorgänge gemäß Art. 42 DSGVO zertifizieren lassen.

Art. 12 Auskunftsanspruch der Betroffenen

1. Betroffene können gemäß Art. 15 DSGVO Auskunft über die beim Unternehmen über sie gespeicherten Daten verlangen. Ihnen wird dann entsprechend ihrer Anfrage Auskunft darüber erteilt, welche personenbezogenen Daten welcher Herkunft über sie zu welchen Zwecken beim Unternehmen gespeichert sind. Im Falle einer (geplanten) Übermittlung wird den Betroffenen auch über die Dritten oder die Kategorien von Dritten, an die seine Daten übermittelt werden (sollen), Auskunft erteilt.

2. Eine Auskunft kann nur unterbleiben, wenn sie die Geschäftszwecke des Unternehmens erheblich gefährden würde, insbesondere wenn aufgrund besonderer Umstände ein überwiegendes Interesse an der Wahrung eines Geschäftsgeheimnisses besteht, es sei denn, dass das Interesse an der Auskunft

die Gefährdung überwiegt oder wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen des überwiegenden rechtlichen Interesses eines Dritten geheim gehalten werden müssen.

3. Vor Erteilung der Auskunft kann das Unternehmen einen Legitimationsnachweis vom Betroffenen darüber verlangen, dass er der Betroffene ist.

Art. 13 Ansprüche auf Berichtigung, Löschung und Sperrung

1. Erweisen sich die gespeicherten personenbezogenen Daten als unrichtig oder unvollständig, werden diese gemäß Art. 16 DSGVO berichtigt bzw. ergänzt.

2. Personenbezogene Daten werden gemäß Art. 17 DSGVO unverzüglich gelöscht, wenn die Erhebung oder Verarbeitung von Anfang an unzulässig war, die Verarbeitung oder Nutzung sich auf Grund nachträglich eingetretener Umstände als unzulässig erweist oder die Kenntnis der Daten für die verantwortliche Stelle zur Erfüllung des Zwecks der Verarbeitung oder Nutzung nicht mehr erforderlich ist.

3. Die Prüfung des Datenbestandes auf die Notwendigkeit einer Löschung nach Absatz 2 erfolgt in regelmäßigen Abständen. Der zeitliche Abstand zwischen Prüfungsintervalle richten sich nach der Sensibilität der Daten.

4. An die Stelle einer Löschung tritt eine Sperrung gemäß Art. 18 DSGVO, soweit der Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten entgegenstehen, Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt würden oder die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Personenbezogene Daten werden ferner gesperrt, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen lässt.

5. Im Falle der Weiterleitung von personenbezogenen Daten benachrichtigt das Unternehmen die empfangenden Stellen über eine erforderliche Berichtigung, Löschung oder Sperrung der Daten.

6. Soweit die Berichtigung, Löschung oder Sperrung der Daten aufgrund eines Antrags der Betroffenen erfolgte, werden diese unverzüglich nach der Ausführung hierüber unterrichtet.

Art. 14 Verantwortlichkeit im Unternehmen

1. Die Unternehmen gewährleisten, dass die Anforderungen des Datenschutzes und der Datensicherheit beachtet werden.

2. Beschäftigte, die mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind, werden mit den rechtlichen Vorschriften und diesen Regeln vertraut gemacht. Sie werden darüber unterrichtet, dass Verstöße gegen datenschutzrechtliche Vorschriften auch als Ordnungswidrigkeit geahndet oder strafrechtlich verfolgt werden und Schadensersatzansprüche nach sich ziehen können. Verletzungen datenschutzrechtlicher Vorschriften, für die einzelne Beschäftigte verantwortlich gemacht werden können, können entsprechend dem jeweils geltenden Recht arbeitsrechtliche Sanktionen nach sich ziehen.

Art. 15 Beauftragte für den Datenschutz

1. Jedes Unternehmen benennt gemäß Art. 37 DSGVO, § 38 Abs, 1 BDSG mindestens einen Beauftragten für den Datenschutz als weisungsunabhängiges Organ, welches auf die Einhaltung der anwendbaren nationalen und internationalen Datenschutzvorschriften sowie dieser Regeln hinwirkt. Die Unabhängigkeit des Datenschutzbeauftragten wird gewährleistet.

2. Die Beauftragten überwachen die ordnungsgemäße Anwendung der im Unternehmen eingesetzten Datenverarbeitungsprogramme und werden zu diesem Zweck vor der Einrichtung oder nicht nur unbedeutenden Veränderung eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten rechtzeitig unterrichtet und wirken hieran beratend mit. Dazu können sie in Abstimmung mit der jeweiligen Unternehmensführung alle Unternehmensbereiche zu den notwendigen Datenschutzmaßnahmen veranlassen. Insoweit haben sie ungehindertes Kontrollrecht im Unternehmen.

3. Die Beauftragten für den Datenschutz machen die bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut.

4. Daneben können sich alle Betroffenen jederzeit mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit auch an die Beauftragten für den Datenschutz wenden. Anfragen, Ersuchen und Beschwerden werden vertraulich behandelt. Die für die Kontaktaufnahme erforderlichen Daten werden in geeigneter Form bekannt gegeben.

5. Die für den Datenschutz verantwortlichen Geschäftsführungen der Unternehmen unterstützen die Beauftragten für den Datenschutz bei der Ausübung ihrer Tätigkeit und arbeiten mit ihnen vertrauensvoll zusammen, um die Einhaltung der anwendbaren nationalen und internationalen Datenschutzvorschriften und dieser Regeln zu gewährleisten. Die Datenschutzbeauftragten können sich dazu jederzeit mit der jeweils zuständigen datenschutzrechtlichen Aufsichtsbehörde vertrauensvoll beraten.

Art. 16 Beschwerden und Reaktion bei Verstößen

1. Die Unternehmen werden Beschwerden von Betroffenen wegen Verstößen gegen datenschutzrechtliche Regelungen gemäß Art. 12 Abs. 3 DSGVO unverzüglich, spätestens innerhalb von einem Monat nach Eingang des Antrags, beantworten. Die für die Kontaktaufnahme erforderlichen Daten werden in geeigneter Form bekannt gegeben. Der verantwortliche Fachbereich hat den Beauftragten für den Datenschutz umgehend zu informieren.

2. Die Geschäftsführungen der Unternehmen werden bei begründeten Beschwerden so schnell wie möglich Abhilfe schaffen. Sollte dies einmal nicht der Fall sein, können sich die Beauftragten für den Datenschutz an die zuständige Aufsichtsbehörde für den Datenschutz wenden. Sie teilen dies den Betroffenen unter Benennung der zuständigen Aufsichtsbehörde mit.

Art. 17 Unrechtmäßige Kenntniserlangung Dritter (Datenpannen)

1. Falls personenbezogene Daten unrechtmäßig übermittelt worden oder Dritten unrechtmäßig zur Kenntnis gelangt sind, informieren die Unternehmen die zuständige Aufsichtsbehörde innerhalb der gesetzlichen Fristen gemäß Art. 33 DSGVO. Die Betroffenen werden benachrichtigt, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind. Würde eine Benachrichtigung unverhältnismäßigen Aufwand erfordern, z. B. wegen der Vielzahl der betroffenen Fälle oder wenn eine Feststellung der Betroffenen nicht in vertretbarer Zeit oder mit vertretbarem technischem Aufwand möglich ist, tritt an ihre Stelle eine Information der Öffentlichkeit.

2. Die Unternehmen verpflichten ihre Auftragsdatenverarbeiter, sie unverzüglich über Vorfälle nach Absatz 1 bei diesen zu unterrichten.

3. Die Unternehmen erstellen ein Konzept für den Umgang mit Vorfällen nach Absatz 1. Sie stellen sicher, dass diese der Geschäftsführung sowie dem betrieblichen Datenschutzbeauftragten unverzüglich zur Kenntnis gelangen.

22.05.2018