Datenschutzkonzept

Klassifizierung:	INTERN
Version:	0.1
Veröffentlicht von:	Geschäftsleitung
Veröffentlicht am:	06.02.2018

Vorwort der Geschäftsführung/ des DSB

>> optional, ggfs einfügen <<

Inhaltsverzeichnis

Dokumentenhistorie

Version	Beschreibung	Bearbeiter	Datum
0.1	Erstellung erster Entwurf		XX.XX.17

1. Einleitung

Das vorliegende Datenschutzkonzept zeigt den ordnungsgemäßen Umgang mit jeglichen Informationen auf, die innerhalb der Unternehmensgruppe Unternehmen XY, aber auch außerhalb der Geschäftsräume, im Sinne der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) verarbeitet werden. Das Datenschutzkonzept leistet damit einen wichtigen Beitrag zum rechtmäßigen Umgang mit personenbezogenen Daten bei allen geschäftlichen Aktivitäten und stellt ein wesentliches Kernelement des Datenschutzmanagementsystems von Unternehmen XY dar.

Die Unternehmen XY sieht den Datenschutz nicht nur als gesetzliche Verpflichtung, sondern als wichtiges Unternehmensziel an. Besonders die personenbezogenen Daten der Kunden sowie der Mitarbeiter erfordern einen aktiven Datenschutz seitens der Unternehmen XY. Alle Kunden und Mitarbeiter müssen sicher sein können, dass ihre Daten bei der Unternehmen XY in guten Händen sind.

Datenschutz ist zuerst Managementverantwortung. Dieser Verantwortung hat sich die Unternehmensleitung gestellt. Da Datenschutz aber nicht (nur) verordnet werden kann, sondern an jedem Arbeitsplatz im Unternehmen gelebt werden muss, unterstützt dieses Datenschutzkonzept alle Mitarbeiter/innen bei der Berücksichtigung des Datenschutzes an ihrem jeweiligen Arbeitsplatz durch konkrete Handlungsanweisungen. Alle Mitarbeiter sind zur Einhaltung und Umsetzung dieses Konzeptes verpflichtet.

1.1. Allgemeine Hinweise zum Datenschutz

Das Datenschutzrecht umfasst ein Regelungswerk zum Umgang mit personenbezogenen Daten, um die Persönlichkeitsrechte der von der Datenverarbeitung betroffenen Personen zu schützen. Es gilt, den „gläsernen Menschen“ zu verhindern und die Persönlichkeitsrechte der betroffenen Personen zu schützen.

Die europäische Datenschutzgrundverordnung (DSGVO), das Bundesdatenschutzgesetz und die weiteren bereichs- und landesspezifischen Regelungen leiten sich aus der europäischen Grundrechtecharta und dem Grundgesetz Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und 10 Abs. 1 GG ab. Dabei wird Datenschutz insbesondere durch das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. In allen Staaten der EU gilt mit der DSGVO ein einheitliches Mindestniveau für Datenschutz. Dieses Datenschutzkonzept soll

insbesondere im Hinblick auf die neuen gesetzlichen Anforderungen der DSGVO einen wesentlichen Beitrag leisten, Compliance in diesem Bereich zu gewährleisten.

1.2. Geltungsbereich

Das vorliegende Datenschutzkonzept stellt die Grundlage zum Umgang mit personenbezogenen Daten dar. Die weiteren existierenden Vorgaben, Pflichten, Richtlinien und Betriebsvereinbarungen zum Umgang mit personenbezogenen Daten gelten ergänzend, soweit sie diesem Konzept nicht widersprechen. Es gilt sowohl für die Verarbeitung von Daten von Privat- und Unternehmenskunden als auch für die Daten von Vertragspartnern, Ansprechpartnern und sonstigen externen Stellen sowie für die Daten von Mitarbeitern, Auszubildenden, Bewerbern oder anderen Personen, ungeachtet der Art des Anstellungsverhältnisses.

Das Datenschutzkonzept gilt für alle Gesellschaften des Unternehmensverbundes. Es richtet sich an sämtliche Mitarbeiter der einzelnen Gesellschaften, unabhängig von der Art des Anstellungsverhältnisses sowie an freie Mitarbeiter, Mitarbeiter auf Zeit sowie sonstige Arbeitskräfte (nachfolgend zusammenfassend auch als „Mitarbeiter" bezeichnet).

1.3. Datenschutz als Marketingfaktor

Aktiver Datenschutz kann als Marketingfaktor eingesetzt werden. Dies gilt gerade vor der gesteigerten Sensibilität der (End)Kunden den Umgang mit ihren personenbezogenen Daten betreffend. Aber auch Auftraggeber legen immer mehr Wert darauf, dass ihre Subunternehmer eine datenschutzrechtliche Compliance und den gesetzlichen Anforderungen entsprechenden Standard an technischen Sicherheitsmaßnahmen aufweisen können. Werden nicht nur die gesetzlichen Verpflichtungen umgesetzt, sondern Datenschutz als wichtiger Bestandteil der Unternehmensphilosophie von Unternehmen XY verstanden, dann kann diese Tatsache gegenüber den Kunden und potentiellen Kunden auch zur positiven Abgrenzung von Mitbewerbern verwendet werden.

1.4. Folgen von Datenschutzverletzungen

Der unrechtmäßige Umgang mit personenbezogenen Daten kann Schadensersatzforderungen der betroffenen Personen nach sich ziehen und zu Imageverlusten führen.

Die hierdurch entstehenden Folgeschäden lassen sich nur schwer beziffern, dürfen aber nicht unterschätzt werden. Ein nachlässiger Umgang mit personenbezogenen Daten kann weiter zu Beschwerden betroffener Personen bei den Aufsichtsbehörden führen.

Darüber hinaus stellt die unzulässige oder unrichtige Verwendung personenbezogener Daten meist auch eine nach der DSGVO mit bis zu 20.000.000 Euro oder 4% des weitweiten Jahresumsatzes Bußgeld bewehrte Ordnungswidrigkeit oder gar eine Straftat dar, die mit bis zu drei Jahren Haft bestraft werden kann.

2. Begriffsdefinitionen

Zentrales Element des Datenschutzrechtes sind die personenbezogenen Daten. Unter diesen Begriff fallen alle Angaben über die persönlichen oder sachlichen Verhältnisse einer Person. Jede Angabe kann daher ein personenbezogenes Datum sein, sofern sie einer konkreten Person zugeordnet werden kann. Banale Angaben gehören ebenso dazu, wie ganz offensichtliche oder öffentlich abrufbare Informationen. Bei einer Statistik, die keine Rückschlüsse auf die einzelnen Personen zulässt, handelt es sich hingegen üblicherweise nicht um personenbezogene Daten.

Einige Informationen über Personen gelten als besonders sensibel. Diese besonderen Kategorien von personenbezogenen Daten umfassen alle Angaben über politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die genetischen Daten, die biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, die Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Sobald sich Angaben über eine Person auf diese Teilbereiche beziehen ist stets höchste Achtsamkeit geboten.

Unter dem Begriff Datenverarbeitung werden alle erdenklichen Schritte im Umgang mit Daten zusammengefasst. Eingeschlossen sind die Erhebung der Daten, die Speicherung, die Übermittlung und Weitergabe, die Veränderung oder Zusammenführung der Daten, die Analyse und sogar deren Löschung oder jede andere Form der Nutzung. Der Begriff ist sehr weit gefasst.

Als betroffene Person wird im Datenschutzrecht diejenige Person bezeichnet, der die personenbezogenen Daten zugeordnet werden können. Es handelt sich also um den von

der Datenverarbeitung Betroffenen. Jeder betroffenen Person stehen bestimmte unabdingbare datenschutzrechtliche Rechte zur Verfügung.

Der Begriff des Verantwortlichen beschreibt das Gegenstück zur betroffenen Person. Der Verantwortliche ist diejenige Gesellschaft, die die Datenverarbeitung steuert, die also bestimmt, in welcher Weise die Daten der betroffenen Person zu verarbeiten sind. Die Verarbeitung kann dabei auch an eine andere Stelle (z.B. eine andere Gesellschaft innerhalb der Unternehmen XY Unternehmensgruppe oder einen externen Dienstleister) ausgelagert werden. Verantwortlicher bleibt jedoch stets der Auftraggeber. Die klare Zuordnung des Verantwortlichen ist entscheidend, weil die betroffenen Personen stets nur einen eindeutigen Ansprechpartner haben sollen.

Im Einzelnen:

Personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Name, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Personenbezogene Daten können beispielsweise folgende Angaben sein:

- Name, Alter, Familienstand, Geburtsdatum, Beruf, Anschrift, Telefonnummer, E-Mail-Adresse
- Angaben zum Einkommen, bevorzugte Zahlungsart, Konto- und Kreditkartennummer, Bonitätseinschätzung, Zahlungsverhalten oder Außenstände
- Kennzahlen (z.B. Kundennummer, Personalnummer)
- Biometrische Daten (z.B. Körpergröße), Gesundheitsangaben (z.B. Vorerkrankungen)
- Verwandtschafts- und soziale Beziehungen
- Kundeneigenschaften (z.B. vorhandene Verträge, Vertragshistorie)
- Konsumgewohnheiten (z.B. Verbrauchsdaten, genutzte Verkehrsmittel, Inhalte von Mülltonnen)
- Surfgewohnheiten (z.B. Angaben zum Browser, Surfhistorie)
- Videoaufzeichnungen und Fotografien

Besondere Kategorien personenbezogener Daten: Daten aus denen die rassische, ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit hervorgehen sowie Daten über die Gesundheit, das Sexualleben einer Person oder deren sexuellen Orientierung.

Verantwortlicher: Ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Verarbeitung: jeden mit oder ohne Hilfe von automatisierten Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Anonyme und pseudonyme Daten: Das Gegenteil eines personenbezogenen Datums wird als anonymes Datum bezeichnet. Anonyme Daten können nicht einer konkreten Person zugeordnet werden. Angaben über die Arbeitslosenquote oder Statistiken über die durchschnittliche Nutzung der öffentlichen Verkehrsmittel lassen keine Aussagen über individuelle Personen zu, diese Angaben sind daher anonym. Da anonyme Daten gerade nicht personenbezogen sind, unterfallen sie nicht dem Datenschutzrecht. Sie können gleichwohl als Unternehmensdaten einer besonderen Vertraulichkeitsstufe unterliegen (z.B. Geschäftszahlen, interne Statistiken). Pseudonyme Daten sehen auf den ersten Blick den anonymen Angaben sehr ähnlich. Den Begriff Pseudonym könnte man mit „Deckname“ übersetzen. Anders als bei anonymen Angaben ist bei der Verwendung eines Pseudonyms eine Zuordnung zu einer konkreten Person jedoch weiterhin möglich. Die Zuordnung erfolgt lediglich über einen Zwischenschritt, beispielsweise einem Abgleich oder einer Suche in einer Kundendatenbank oder einem Mitarbeiterverzeichnis. Pseudonyme Daten sind daher personenbezogene Daten und unterfallen dem Datenschutzrecht.

Beispiel: Bei der Angabe „Der Mitarbeiter mit der Personalnummer 1241 hat im letzten Monat 11,5 Überstunden geleistet“ handelt es sich folglich um ein pseudonymes Datum. Mit den in der Personalabteilung verfügbaren Informationen kann der Personenbezug der Information hergestellt werden. Die Angabe ist daher personenbezogen. Die Angabe „Ein Bundesbürger verbraucht im Durchschnitt 121l Wasser“ kann nicht auf eine konkrete Person bezogen werden. Es handelt sich nicht um ein personenbezogenes Datum.

3. Rollen und Verantwortlichkeiten

Für die Umsetzung des Datenschutzkonzeptes im alltäglichen Geschäftsbetrieb sind die Geschäftsführung sowie in den einzelnen Unternehmensbereichen jeweils die von der Geschäftsführung eingesetzten Leitungspersonen verantwortlich. Datenschutz richtet sich jedoch ausdrücklich an alle Mitarbeiter, so dass alle Mitarbeiter bei der Unternehmen XY für den Schutz von personenbezogenen Daten sorgen müssen.

3.1 Geschäftsführer

>> einfügen <<

3.2 Leitungspersonen

>> einfügen <<

Bereich	Name/Position
Legal	
IT	
Operations	
Finance	
Marketing/Sales	

3.3. Verantwortlicher

Der Begriff des Verantwortlichen dient als Anknüpfungspunkt für die gesetzlich festgelegten Rechte und Pflichten. Gegenstand der Verantwortlichkeit ist der Datenumgang. Verantwortlicher im Hinblick auf den in diesem Datenschutzkonzept beschriebenen Datenumgang ist die

>> einfügen <<

4. Datenschutzrechtliche Einordung von Unternehmen XY

Für die Unternehmen XY gilt in erster Linie die DSGVO sowie das BDSG.

>> Hier eine Beschreibung der Hauptzwecke der Verarbeitung einfügen.<<

5. Betrieblicher Datenschutzbeauftragter

Die Unternehmen XY hat nach Maßgabe des § 38 BDSG, Art. 37 DSGVO einen betrieblichen Datenschutzbeauftragten (DSB) bestellt.

Es handelt sich um: >> <<

Dieser nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seiner Fachkunde wahr. Die Fachabteilungen stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen.

Jeder Mitarbeiter von der Unternehmen XY kann sich unmittelbar mit Fragen, Hinweisen, Anregungen oder Beschwerden an den DSB wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

6. Datenschutzrechtliche Rahmenbedingungen

Für die Unternehmen XY gelten folgende datenschutzrechtliche Rahmenbedingungen:

6.1. Rechtsgrundlagen der Verarbeitungen

Für die Verarbeitung personenbezogener Daten gilt das sogenannte Verbot mit Erlaubnisvorbehalt, was sich sowohl in der DSGVO als auch im BDSG wiederfindet. Das bedeutet konkret, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, es sei denn, sie ist ausdrücklich erlaubt.

Nach Art. 6 DSGVO und den vergleichbaren bereichsspezifischen Regelungen ist die Verarbeitung personenbezogener Daten nur dann erlaubt, wenn

- die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecken gegeben hat,
- die Verarbeitung für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist,
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist,

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

Es wird bei der Verarbeitung personenbezogener Daten sichergestellt, dass für jede Verarbeitung der entsprechende Erlaubnistatbestand gegeben ist. Dies ist etwa im Hinblick auf die Verarbeitung von Mitarbeiterdaten Art. 88 DSGVO, § 26 BDSG und für die Verarbeitung bestimmter Kundendaten der bereits genannte Art. 6 DSGVO.

Für jede Datenverarbeitung für die keiner der gesetzlichen Erlaubnistatbestände greift, wird sichergestellt, dass eine wirksame Einwilligung der betroffenen Person eingeholt wird. Das Verbot der ausschließlich automatisch erfolgenden Verarbeitung personenbezogener Daten bei der diese Verarbeitung rechtliche oder ähnliche Wirkung für die betroffenen Personen entfaltet wird beachtet.

6.2. Einwilligung der betroffenen Person

Neben der gesetzlichen Erlaubnis zur Datenverarbeitung stellt die Einwilligung der betroffenen Person nach Art. 6 Abs. 1 a DSGVO eine Möglichkeit dar, um zulässige Datenverarbeitung zu betreiben. Die DSGVO und die Rechtsprechung stellen an die Einwilligung strenge Anforderungen, die in Art. 7 DSGVO geregelt sind. Die Einwilligung des Betroffenen muss demnach freiwillig und informiert erfolgen. Dies stellt Unternehmen XY beispielsweise in Bezug auf die Einwilligung in die Speicherung der Daten von Bewerbern über den Bewerbungsprozess hinaus (in einem Bewerber-Pool), sicher.

6.3. Zweckbindung

Der Zweck der Datenverarbeitung folgt aus der jeweiligen Fachaufgabe, zu deren Erfüllung die Daten erhoben wurden. Die Zwecke der Datenverarbeitung müssen eindeutig und legitim sein und zum Zeitpunkt der Erhebung der Daten feststehen. Das Datenschutzrecht verlangt, dass alle personenbezogenen Daten grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie ursprünglich erhoben wurden. Jedes Datum dient einem bestimmten Zweck und es kann grundsätzlich keine personenbezogenen Daten im Unternehmen geben,

die „frei" für alle erdenklichen Zwecke genutzt werden dürfen. Daten, die nicht mehr für ihre ursprünglichen Zwecke benötigt werden, sind grundsätzlich zu löschen, wenn das Gesetz nicht ausdrücklich die weitere Aufbewahrung verlangt.

Eine Datenverarbeitung zu einem anderen als dem ursprünglich festgelegten Zweck ist als Zweckänderung oder Zweckdurchbrechung gemäß Art. 6 Abs. 4 DSGVO nur auf gesetzlicher Grundlage oder mit Einwilligung der betroffenen Person zulässig. Dies gilt auch dann, wenn die Daten an eine andere Stelle mit einer anderen, über bloße Hilfsfunktionen hinausgehenden Aufgabenstellung weitergegeben werden sollen.

Es wird in sämtlichen Prozessen bei der Unternehmen XY sichergestellt, dass personenbezogene Daten nur zu dem Zweck verarbeitet werden, zu dem sie erhoben werden, bzw. eine gesetzliche Erlaubnis vorliegt oder eine ausdrückliche Einwilligung der betroffenen Person eingeholt wird sofern eine Zweckänderung vorgesehen ist.

6.4. Richtigkeit

Die Unternehmen XY trägt dafür Sorge, dass die in der Unternehmensgruppe gespeicherten Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind.

6.5. Datenminimierung

Der Grundsatz der Datenminimierung bedeutet, dass nur so viele und nur solche Daten erhoben und verarbeitet werden dürfen, die für die jeweilige Anwendung unbedingt erforderlich sind. Dies wird von der Unternehmen XY in allen Prozessen berücksichtigt in denen personenbezogene Daten verarbeitet werden.

6.6. Transparenz

Die betroffene Person hat stets das Recht über die zu seiner Person gehörenden Daten zu verfügen. Er muss verstehen können, wer welche Daten über seine Person zu welchen Zwecken speichert und verarbeitet. Über die Zwecke der Verarbeitung ist die betroffene Person spätestens im Zeitpunkt der Erhebung zu informieren. Datenverarbeitung darf daher nie heimlich und ohne das Wissen der betroffenen Person stattfinden. Um die Transparenz zu wahren ist es entscheidend, die Schritte der Datenverarbeitung sorgfältig zu erläutern (beispielsweise in der Datenschutzerklärung) und alle Anfragen zum Datenschutz ernsthaft, vollständig und wahrheitsgetreu zu beantworten. So regelt Art. 13 DSGVO, dass den betroffenen Personen v.a. die Kontaktdaten des Verantwortlichen der verarbeitenden Stelle, der Zweck (für jede einzelne Datenverarbeitung gesondert) und die Dauer der

Datenverarbeitung sowie Auskunfts- und Widerspruchsrechte ebenso wie die Rechtsgrundlage der Datenverarbeitung und eine nachvollziehbare Interessenabwägung mitgeteilt werden. Allgemein müssen die betroffenen Personen über alle Rechte informiert werden, also über das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und auf Datenübertragbarkeit. Zudem müssen die betroffenen Personen darüber informiert werden, inwieweit die Entscheidungsfindung ausschließlich auf einer automatischen Datenverarbeitung (v.a. Profiling) beruht.

Dabei ist zu berücksichtigen, dass der betroffenen Personen die Informationen sofort bei Datenerhebung übermittelt werden. Dabei verlangt Art. 12 DSGVO, dass diese Informationen der betroffenen Person in „transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" vorgelegt werden. Dabei lässt die DSGVO eine mündliche, schriftliche oder auch elektronische Übermittlung der Informationen genügen. Besonders gegenüber Kindern ist auf die Verständlichkeit der Informationen zu achten. Die Informationspflicht besteht nur dann nicht, wenn die betroffene Person im Falle einer Datenverarbeitung bereits über die erforderlichen Informationen verfügt. Hierfür trägt die Unternehmen XY die Beweislast.

6.7. Sicherheit

Die Unternehmen XY muss nachweisbar dafür sorgen, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit für diese Daten gewährleistet. Dies ist durch die implementierten technischen und organisatorischen Maßnahmen gewährleistet.

6.8. Datenschutzfolgeabschätzung

Nach Artikel 35 DSGVO besteht die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung. Damit wird eine Risikoeinschätzung bezeichnet, die Unternehmen XY vor der Verarbeitung personenbezogener Daten vornehmen muss. Eine Datenschutz-Folgenabschätzung ist grundsätzlich nur durchzuführen, wenn ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Dies kann beispielsweise bei folgenden Verfahren der Fall sein:

- Daten zur Bewertung, zum Scoring oder zum Profiling, insbesondere in den Bereichen Arbeit, wirtschaftliche Situation, Gesundheit, persönliche Vorlieben und Interessen, Bonität, Verhaltensweisen, Aufenthaltsort;

- Formen automatisierter Entscheidungsfindung mit rechtlichen Folgen;
- Verarbeitung sensibler Daten wie beispielsweise Gesundheitsdaten;
- umfangreiche Verarbeitungsvorgänge;
- zusammengeführte oder kombinierte Datensätze;
- Daten schutzbedürftiger Personen wie Kindern, älteren Menschen, Patienten oder Mitarbeitern;
- Nutzung neuer Technologien wie IoT-Entwicklungen

Sofern eine Datenschutzfolgeabschätzung gemäß Art. 35 DSGVO erforderlich ist, wird der DSB eingeschaltet. Daher sollen die Mitarbeiter bei der Unternehmen XY dem DSB unverzüglich die Einführung neuer Systeme zur Verarbeitung personenbezogener Daten vorab anzeigen, damit dieser die datenschutzrechtliche Zulässigkeit prüfen kann.

>> ggfs Prozess anpassen, auf RL verweisen <<

Achtung: bei riskanter Datenverarbeitung ist die Konsultationspflicht nach Art. 36 DSGVO zu beachten. Sofern also die Datenschutzfolgenabschätzung ergibt, dass die Datenverarbeitung ein hohes datenschutzrechtliches Risiko mit sich bringt, wird der DSB bzw. die Geschäftsleitung mit der Aufsichtsbehörde in Verbindung treten.

7. Meldepflichten nach der DSGVO

Für die Unternehmen XY hat der Schutz personenbezogener Daten höchste Priorität. Sollte es dennoch einmal zu einer Verletzung des Schutzes personenbezogener Daten kommen ist sich die Unternehmen XY seiner Meldepflicht bewusst und kommt dieser ohne zu Zögern nach. Eine solche Verletzung ist gegeben bei einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zu unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Mit anderen Worten ein unbefugter Datenzugriff, eine „Datenpanne“.

Die DSGVO regelt in Art. 33 und 34 wie bei solchen Datenpannen vorzugehen ist. So hat eine Meldung an die Aufsichtsbehörde grundsätzlich immer zu erfolgen. Eine Ausnahme gilt nur dann, wenn die Datenpanne voraussichtlich nicht zu einem Risiko für die betroffene Person

führt. Bei einer Datenpanne haben die Mitarbeiter von der Unternehmen XY daher unverzüglich den DSB zu informieren, der dann die Bewertung des Risikos für die von der Datenpanne betroffenen Personen vornimmt. Die betroffenen Personen selbst müssen nur dann informiert werden, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht. Zwar kann unter Umständen auf eine Information der betroffenen Personen auch verzichtet werden, sofern technische und organisatorische Maßnahmen gegeben sind, die den Zugriff auf die personenbezogenen Daten durch den Unbefugten verhindern, jedoch ist diese Einschätzung dem DSB zu überlassen.

Da die Meldung der Datenpanne innerhalb 72 Stunden bei der zuständigen Aufsichtsbehörde zu erfolgen hat, sollen die Mitarbeiter nicht zögern, jede Datenpanne dem DSB unverzüglich mitzuteilen.

8. Datenweitergabe an Dritte

Die Weitergabe von Daten an andere Stellen, wie z.B. externe Dienstleister, Behörden, Polizei oder Staatsanwaltschaft sind stets datenschutzrechtlich relevante Vorgänge, die in jedem Einzelfall einer sachgerechten Rechtfertigung bedürfen. Daher muss jede Datenweitergabe kritisch geprüft werden und darf nur mit Freigabe der Vorgesetzten oder des Datenschutzbeauftragten erfolgen.

8.1. Weitergabe innerhalb des Konzerns

Auch die Weitergabe von Daten an eine andere Gesellschaft innerhalb des Unternehmensverbundes der Unternehmen XY muss geprüft werden. Daten dürfen nicht ohne Weiteres zwischen den Gesellschaften übermittelt, zusammengeführt, abgeglichen oder in sonstiger Weise weitergegeben werden. Ein umfassendes Konzernprivileg gibt es nicht. Übermittlungen müssen auch innerhalb von der Unternehmen XY im Rahmen einer Interessensabwägung gerechtfertigt werden.

Da stets nur diejenige Abteilung Zugriff auf die Daten haben darf, die sie für die ihr übertragenen Aufgaben benötigt, ist auch eine Weitergabe innerhalb einer der Gesellschaften nur dann zulässig, wenn in dem betreffenden Einzelfall eine rechtliche Grundlage hierfür besteht. Unternehmen müssen jedes Verfahren einzeln auf Rechtmäßigkeit prüfen und mit den Interessen der betroffenen Personen abwägen.

Die Datenweitergabe innerhalb der Konzernstrukturen bei der Unternehmen XY wird durch entsprechende datenschutzrechtliche Verträge (sofern erforderlich) flankiert, um die Rechtmäßigkeit der Verarbeitung sicherzustellen.

8.1. Externe Dienstleister und Auftragsverarbeitung

Wenn die Inanspruchnahme einer externen Dienstleistung vorgesehen ist, bei der bei Unternehmen XY gespeicherte personenbezogene Daten an den Dienstleister übermittelt werden müssen oder der Dienstleister Zugriff auf gespeicherte personenbezogene Daten erhält, hat der Verantwortliche des entsprechenden Bereichs sicherzustellen, dass der Datenschutzbeauftragte informiert wird und ggf. ein Auftragsverarbeitungsvertrag geschlossen wird.

>> ggfs Prozess anpassen, auf RL verweisen <<

Darüber hinaus müssen Besonderheiten von Datenverarbeitungen oder -übermittlungen in sog. unsichere Drittländer (wie die USA) beachtet werden und ggf. ergänzende Vereinbarungen getroffen werden.

Wenn die Inanspruchnahme einer externen Dienstleistung vorgesehen ist, bei der bei der Unternehmen XY gespeicherte personenbezogene Daten an den Dienstleister (Auftragsverarbeiter) übermittelt werden müssen oder der Dienstleister Zugriff auf personenbezogene Daten erhält, so ist hierfür ein schriftlicher Vertrag erforderlich. Der Auftragsverarbeiter muss sorgfältig und unter Berücksichtigung der technischen und organisatorischen Maßnahmen ausgewählt werden und darf die Daten nur entsprechend der Weisung von der Unternehmen XY verarbeiten. Die von Art. 28 Abs. 3 DSGVO aufgestellten inhaltlichen Anforderungen an einen solchen Vertrages sind zu beachten. Um dies zu gewährleisten soll der DSB über die Absicht einen Vertrag über Auftragsdatenverarbeitung zu schließen informiert werden.

9. Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Alle Mitarbeiter bei der Unternehmen XY werden im Rahmen der Unterzeichnung des Arbeitsvertrages über die Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes belehrt und unterzeichnen eine entsprechende Erklärung welcher der Personalakte beigefügt wird.

Darüber hinaus werden regelmäßige Datenschutzschulungen bei der Unternehmen XY durchgeführt.

>> ggfs anpassen, ausführlichere Beschreibung <<

10. Beschreibung der personenbezogenen Daten und Zweckbindung

Bei der Unternehmen XY werden folgende personenbezogene Daten bzw. Datenkategorien verarbeitet:

>> ggfs. anpassen und detaillieren <<

10.1. Bewerberdaten

Bei dem betroffenen Personenkreis handelt es sich um Bewerber und Interessenten an Vakanzen.

Die Daten betreffen Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Bewerber, die im Laufe des Bewerbungsverfahrens mitgeteilt werden. In der Regel handelt es sich um folgende Daten:

- Name
- Adressdaten
- Geburtsdatum
- Lichtbild
- Name der Eltern/ Geburtsdatum/ Beruf/ religiöse oder politische Überzeugung (diese Angaben werden nicht gefordert, werden aber häufig unaufgefordert mitgeteilt)
- Bildungsweg: Abschlussnoten und Bildungseinrichtungen
- Angaben zu ehemaligen Arbeitgebern, Referenzen und Arbeitszeugnisse
- Angaben zu aktuellen Kündigungsfristen, Gehaltsvorstellungen und zeitlichen Verfügbarkeiten
- Bei Bewerbern aus Drittstaaten: Art und Laufzeit der vorliegenden Arbeits- und Aufenthaltserlaubnis
- Kopie des Passes

Die Daten werden genutzt für das Bewerbermanagement.

10.2. Mitarbeiterdaten

Bei dem betroffenen Personenkreis handelt es sich um Mitarbeiter (Festangestellte, Werkstudenten, Praktikanten) und Freelancer.

Die Daten betreffen Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Mitarbeiter. In der Regel handelt es sich um folgende Daten:

- Name und Geburtsname
- Adressdaten (aktuelle Meldeadresse)
- Geburtsdatum
- Kontoverbindung
- Steuernummer, Steuerklasse, Religionszugehörigkeit, Familienstand, Nationalität
- Ausbildungsgrad
- Krankenkassen- und Rentenversicherungsdaten
- Joblevel, Gehalt
- Handynummer, Festnetznummer, private E-Mailadresse (freiwillig), Notfallkontakt (Name und Telefonnummer, freiwillig)
- in Spezialfällen: Kopie des Passes (Aufenthaltstitel bei Mitarbeitern aus Drittstaaten)
- tätigkeitsbezogene Mitarbeiterdaten, bspw. Lohnbuchhaltungsdaten, Spesenabrechnungen, Urlaubs- und Krankenzeiten, Arbeitszeiterfassung, Abmahnungen, Beurteilungen

Die Daten werden genutzt für die Abwicklung der Arbeitsverhältnisse und für die Anmeldung der Mitarbeiter bei Finanzämtern, Krankenkassen und der Rentenversicherung.

10.3. Accountingdaten

Bei dem betroffenen Personenkreis handelt es sich um die Mitarbeiter der Buchhaltung und der Finanzabteilung sowie um Lieferanten und Kunden.

Die Daten betreffen Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Mitarbeiter, Lieferanten und Kunden. In der Regel handelt es sich um folgende Daten:

Mitarbeiter der Buchhaltung und der Finanzabteilung

- Namen der Ansprechpartner
- Adressdaten der Ansprechpartner
- Rechnungsinformationen inkl. Steuernummern und Kontoverbindungen

Lieferanten

- Namen der Ansprechpartner
- Adressdaten
- Rechnungsinformationen inkl. Steuernummern und Kontoverbindungen

Kunden

- Namen der Ansprechpartner
- Adressdaten/ E-Mail-Adressen
- Kommunikationsinhalte

Die Daten werden genutzt für Accountingzwecke.

10.4. Nutzungsdaten

Bei dem betroffenen Personenkreis handelt es sich um Nutzer der Unternehmen XY-Website - www.Unternehmen-XY.com.

>> ggfs. anpassen und detaillieren <<

Die Daten betreffen Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Nutzer. In der Regel handelt es sich um folgende Daten:

Nutzungsdaten im Sinne des § 15 Abs. 1 TMG, bspw.:

- IP-Adresse des anfragenden Rechners
- Datum und Uhrzeit des Zugriffs
- Name und URL der abgerufenen Datei
- übertragene Datenmenge
- Meldung, ob der Abruf erfolgreich war
- Erkennungsdaten des verwendeten Browsers und Betriebssystems

Die Daten werden genutzt, um dem Nutzer die Inanspruchnahme der Unternehmen XY-Website zu ermöglichen sowie für Zwecke der Werbung, der Marktforschung und zur bedarfsgerechten Gestaltung der Unternehmen XY-Website.

10.5. Kundendaten

Bei dem betroffenen Personenkreis handelt es sich Kunden von Unternehmen XY. Überwiegend ist die Unternehmen XY im Bereich Business to Business tätig, so dass personenbezogenen Daten in diesem Kontext nur in geringem Maße betroffen sind, wie etwa Namen und E-Mail-Adresse von Ansprechpartnern:

- Namen der Ansprechpartner
- Adressdaten/ E-Mail-Adressen
- Kommunikationsinhalte

10.6. Besondere Kategorien von personenbezogenen Daten

Besondere Arten personenbezogener Daten sind gemäß Art. 9 Abs. 1 DSGVO Daten, die Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben oder sexuellen Orientierung enthalten. Darüber hinaus fallen unter den Begriff genetische und biometrische Daten.

In folgenden Fällen kann es im Geschäftsbetrieb von der Unternehmen XY zu einem Umgang mit besonderen Kategorien personenbezogener Daten kommen:

- Verarbeitung Mitarbeiterdaten (Gesundheit, Religion)
- Verarbeitung Bewerberdaten (Gesundheit, religiöse oder weltanschauliche Überzeugungen)

11. Gewährleistung von Rechten der betroffenen Personen

Den betroffenen Personen stehen Ansprüche auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und auf Datenübertragbarkeit zu.

Die Unternehmen XY stellt sicher, dass alle im Rahmen eines berechtigten Ersuchens benötigten Daten schnell und vollständig innerhalb eines Monats zur Verfügung stehen. Die Persönlichkeitsrechte Dritter sind dabei zu wahren.

11.1. Auskunft

Betroffene Personen haben nach Art. 15 DSGVO gegenüber dem Verantwortlichen ein Recht auf Auskunft darüber, welche Daten zu ihrer Person gespeichert werden, zu welchem Zweck die Daten gespeichert werden sowie über die Empfänger und die Herkunft der Daten.

Es ist hierbei von oberster Priorität, die betroffene Person sicher zu identifizieren, da es einen schweren datenschutzrechtlichen Verstoß bedeuten würde, wenn einem Kunden/Mitarbeiter versehentlich die Informationen über einen anderen Kunden/Mitarbeiter mitgeteilt würden. Die Auskunft erfolgt grundsätzlich unentgeltlich, sie muss außerdem vollständig und wahrheitsgemäß sein.

11.2. Berichtigung

Nach Art. 16 DSGVO hat die betroffene Person das Recht unverzüglich die Berichtigung der ihn betreffenden unrichtigen personenbezogenen Daten zu verlangen. Die Unternehmen XY wird unrichtige personenbezogene Daten auf Verlangen unverzüglich korrigieren.

11.3. Einschränkung der Verarbeitung

Daten dürfen gem. Art. 18 DSGVO dann nicht mehr verarbeitet werden, wenn die betroffene Person die Richtigkeit der Daten bestreitet, die Verarbeitung rechtswidrig ist aber der Betroffene eine Löschung der Daten ablehnt, der Betroffene die Daten noch für die Verfolgung von Rechtsansprüchen benötigt oder der Betroffene Widerspruch gegen die Verarbeitung eingelegt hat und über diesen noch nicht entschieden ist. Die Unternehmen XY wird die Verarbeitung aber auch dann einschränken, wenn zwar die Speicherung aber nicht mehr die Verarbeitung noch zulässig ist.

11.4. Löschung

Gemäß Art. 17 DSGVO hat die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, Darüber hinaus ist der Verantwortliche verpflichtet, personenbezogene Daten unverzüglich zu löschen, wenn einer der folgenden vier Gründe eingreift:

- Das Speichern der Daten ist zur Zweckerreichung der Datenerhebung nicht mehr notwendig
- Die betroffene Person widerruft ihre Einwilligung in die Datenverarbeitung
- Die Daten wurden unrechtmäßig verarbeitet
- Die Unternehmen XY ist aufgrund einer gesetzlichen Pflicht zur Löschung der Daten verpflichtet

Die Unternehmen XY muß das Recht auf Löschung nicht umsetzen, wenn:

- Die Meinungs- und Informationsfreiheit überwiegen
- Das Speichern der Daten einer rechtlichen Verpflichtung entspricht
- Das öffentliche Interesse im Bereich der öffentlichen Gesundheit überwiegt

- Wissenschaftliche oder historische Forschungszwecke oder Archivzwecke überwiegen
- Die Daten zur Wahrung von Rechtsansprüchen erforderlich sind

Sofern die Löschung im Falle nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und das Interesse der betroffenen Person an der Löschung als gering anzusehen ist, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung nicht. In diesem Fall beachtet die Unternehmen XY jedoch die Einschränkung der Verarbeitung gem. Art. 18 DSGVO (s.o.). Jedoch sollte der Datenschutzbeauftragte hier kontaktiert werden.

11.5. Datenübertragbarkeit

Die DSGVO regelt in Art. 20 Abs. 1 das Recht der Datenübertragbarkeit. Dies umfasst zum einen das Recht, eine Bereitstellung des eigenen Datensatzes zu verlangen als auch das Recht, diesen an einen anderen Verantwortlichen zu übermitteln. Die Unternehmen XY stellt den betroffenen Personen den sie betreffenden Datensatz in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung. Will die betroffene Person diesen Datensatz an einen anderen Verantwortlichen übermitteln, so wird die Unternehmen XY die Übermittlung nicht erschweren oder behindern.

11.6.Widerspruch

Betroffene Personen können jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Abs. 1 e oder f DSGVO erfolgt, Widerspruch einlegen. Wurden Daten entsprechend einer dieser beiden Voraussetzungen rechtmäßig erhoben, kann die betroffene Person jederzeit gegen die Verarbeitung dieser Daten Widerspruch einlegen, obwohl die Datenerhebung rechtmäßig war. Die Unternehmen XY wird einen solchen Widerspruch beachten und die Datenverarbeitung einstellen, sofern sich das Widerspruchsrecht aus der „besonderen Situation“ der betroffenen Person ergibt. Diese hat dabei nicht nur das Vorliegen der besonderen Situation, sondern auch das „Überwiegen“ nachzuweisen.

Art. 21 Abs.2 DSGVO gewährt ein jederzeit unentgeltlich ausübbares Widerspruchsrecht, falls die Verarbeitung der personenbezogenen Daten der betroffenen Person im Zusammenhang mit Direktwerbung erfolgt. Die Unternehmen XY wird einen solchen Widerspruch beachten und die Datenverarbeitung einstellen.

12. Verzeichnis von Verarbeitungstätigkeiten/ Dokumentationspflichten

Für automatisierte Verfahren sind Übersichten über folgende Angaben zu machen:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
- Rechtsgrundlage der Datenerhebung, -verarbeitung oder -nutzung,
- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
- Regelfristen für die Löschung der Daten,
- eine geplante Datenübermittlung in Drittstaaten,
- eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind,
- der Zweck der Datenerhebung,
- der wesentliche Inhalt,
- eine Beschreibung der betroffenen Personengruppen,
- die Regelfristen für die Löschung,
- die Angaben zur Art der Verarbeitung sowie den Schutzmaßnahmen.

Es liegen die erforderlichen Verfahrensübersichten bei der Unternehmen XY vor.

13. Technische und organisatorische Maßnahmen zum Datenschutz

Gemäß Art. 32 DSGVO sind technische und organisatorische Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind um ein dem Risiko angemessenes Schutzniveau zu gewährleisten,

In Art. 32 DSGVO findet sich eine nicht abschließende Aufzählung verschiedener technischer und organisatorischer Maßnahmen. Dabei handelt es sich um einen Mindestmaßnahmenkatalog der konkret zu treffende und abstrakte, Zielvorgaben ähnelnde, Maßnahmen enthält. Da es sich um Mindestvorgaben handelt, hängen die Maßnahmen vom Einzelfall ab und sind nicht immer zwingend geboten. Der Maßnahmenkatalog umfasst

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten: Durch die Pseudonymisierung soll der Rückschluss auf eine bestimmte Person nur unter „Hinzuziehung zusätzlicher Informationen", etwa eines Identifizierungsschlüssel, möglich sein. Bei der Verschlüsselung bleibt der Personenbezug dagegen vollständig erhalten jedoch werden die Daten so verändert, dass sie ohne Aufhebung der Verschlüsselung nicht mehr lesbar sind,

- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste: Verhindert werden soll der Zugriff Dritter, erfasst sind aber auch technische Gesichtspunkte wie etwa die Vermeidung der Überlastung informationstechnischer Systeme. Die zu treffenden Maßnahmen hängen dabei vom beabsichtigten Schutzzweck ab, so kann die Vertraulichkeit etwa durch Zutritts-, Zugriffs- oder Zugangskontrolle gewährleistet werden. Zum Schutz der Integrität sollten elektronische Signaturen verwendet werden und die Verfügbarkeit der Datensysteme wird von Unternehmen XY durch Investitionen in Doppelt- oder sogar Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung gewährleistet,

- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen: Neben der Mehrfachvorhaltung von Datenbeständen betrifft dieser Punkt vor allem technische und organisatorische Maßnahmen derart, dass Vertretungspläne für Personalausfälle geschaffen werden oder Stromausfälle durch Notstromversorgung abgefangen werden können,

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung: Gewährleistet werden muss, dass die genannten Sicherheitsmaßnahmen regelmäßig kritisch begutachtet und überprüft werden. Hierzu sollen intern oder extern Prüfberichte erstellt und ausgewertet werden. Gegebenenfalls sollten sich hieran geeignete Maßnahmen anschließen.

Für die Unternehmen XY hat die Umsetzung technischer und organisatorischer Maßnahmen zum Schutz der Daten höchste Priorität. Dies nicht nur zum Schutz unserer Mitarbeiter und Kunden sondern auch um wirksam gegen Wirtschaftsspionage vorzugehen.

13.2. Von der Unternehmen XY getroffene technische und organisatorische Maßnahmen

13.2.1. Maßnahmen zur Pseudonymisierung

>> anpassen und detaillieren <<

13.2.2. Maßnahmen zur Verschlüsselung

>> anpassen und detaillieren <<

13.2.3. Maßnahmen zur Sicherung der Vertraulichkeit

>> anpassen und detaillieren <<

13.2.4. Maßnahmen zur Sicherung der Integrität

>> anpassen und detaillieren <<

13.2.5. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

>> anpassen und detaillieren <<

13.2.6. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Verarbeitung

>> anpassen und detaillieren <<

13.3. Informationssicherheits-Management

Die Unternehmen XY stützt den Schutz von Informationen und insbesondere personenbezogenen Daten auf ein Informationssicherheits-Managementsystem (ISMS), das auf den Standards ISO/IEC 27001:2013(E) und ISO/IEC 27002:2013(E) basiert und sich im Hinblick auf die Handlungsempfehlungen in Teilen an den BSI IT-Grundschutz-Katalogen orientiert. Einzelheiten ergeben sich aus >> anpassen und detaillieren <<

13.4. Klassifizierung nach Schutzbedarf

Zum Schutz von Informationen und insbesondere personenbezogenen Daten erfolgt bei der Unternehmen XY eine Klassifizierung anhand des Schutzbedarfs. Die Kategorien anhand derer Informationen sichtbar gekennzeichnet werden lauten: „öffentlich“, „intern“, „vertraulich“ und „geheim“. Vereinzelt finden sich noch die Klassifizierungen „streng vertraulich“ oder „streng geheim“, diese sind jeweils der Kategorie „geheim“ zuzuordnen.

Sofern Dokumente nicht klassifiziert wurden, sind diese als „intern“ zu behandeln. Einzelheiten ergeben sich aus dem Dokument ….

>> anpassen und detaillieren <<

14. weitere Bestandteile des Datenschutzkonzepts

Weitere Bestandteile des Datenschutzkonzepts sind folgende Richtlinien und Betriebsvereinbarungen:

- Richtlinie zur Nutzung der Kommunikationsmedien
- >> anpassen und detaillieren <<
-