DATENSCHUTZ

STATUS

Konzernrichtlinie ID, Revision:	ID 037, Rev. 00
Datum der Freigabe:	02.05.2018
Geltungsbereich:	Alle Konzerneinheiten
Verfasser:	Alfred Altersberger/Volker Springer
Herausgeber:	BRVZ/CML
Freigegeben durch:	Vorstand der STRABAG SE

I. Zweck und Ziel

Vor dem Hintergrund der voranschreitenden Digitalisierung – unter anderem in Bezug auf das Bauen mit BIM, den Einsatz von mobilen Devices zur Datenverarbeitung, Drohnen und Cloud-Services – werden für uns alle Chancen zur effektiveren Arbeit auf der Baustelle und im Büro eröffnet. Uns ist bewusst, dass diese Entwicklung auch neue Risiken für den Konzern und jede Einzelne/jeden Einzelnen birgt. Aus diesem Grund ist uns Datenschutz – vor allem der Schutz der personenbezogenen Daten – ein maßgebliches Anliegen.

STRABAG bekennt sich zu ihrer Verantwortung für den sorgsamen Umgang mit personenbezogenen Daten. Daher ist ein wesentliches Ziel dieser Richtlinie, ein einheitlich hohes Datenschutzniveau für den Konzern zu gewährleisten.

Diese Richtlinie orientiert sich an den Vorgaben der EU-Datenschutz-Grundverordnung (im Weiteren „DS-GVO“), die mit 25.05.2018 in Kraft tritt und eine umfassende Verschärfung des Datenschutzrechtes mit sich bringt. Auswirkungen ergeben sich insbesondere auf den Umgang mit personenbezogenen Daten. Es werden sowohl Auskunfts-, Informations-, Einwilligungs- und Widerspruchsrechte der Betroffenen gestärkt, als auch die Sanktionierungsmöglichkeiten im Falle der Nichteinhaltung der umfangreichen Anforderungen empfindlich verschärft (bis zu 4 % des Konzernumsatzes!). Weiters bestehen nunmehr nicht nur umfangreiche Dokumentationspflichten zu Anwendungen, die personenbezogene Daten verarbeiten, sondern auch Meldepflichten an Aufsichtsbehörden im Falle von Datenpannen (innerhalb von 72 Stunden). Ebenso sind in bestimmten Fällen Datenschutz-Folgeabschätzungen zu tätigen und bei Abschluss von Dienstleistungsverträgen mit Subunternehmern Mindestinhalte nach DS-GVO zu regeln.

Die Vorgaben gelten für alle Konzerngesellschaften, unabhängig davon, ob sie innerhalb oder außerhalb des Anwendungsbereiches der DS-GVO gelegen sind, es sei denn, länderspezifisch werden höhere Anforderungen gestellt; dann gelten selbstverständlich diese.

Die Umsetzung der sich aus dieser Richtlinie, der DS-GVO und den nationalen Datenschutzvorschriften ergebenden Verpflichtungen ist durch die Führungskräfte und die von ihnen beauftragte Datenschutzorganisation sowie Mitarbeiterinnen/Mitarbeiter im Unternehmen sicherzustellen.

Die Beachtung dieser Richtlinie ist Voraussetzung für den sicheren Austausch von personenbezogenen Daten innerhalb des Konzerns und mit Dritten.

Die Richtlinie ist Teil des umfassenden Datenschutzmanagementsystems (im Folgenden „DSMS“) des Konzerns. Dieses System ist umfassend im STRAnet unter der Rubrik „Datenschutz“ dargestellt.

II. Anwendungsbereich

Diese Richtlinie gilt für jegliche Verarbeitung personenbezogener Daten in und zwischen einzelnen Konzerngesellschaften. Sie regelt umfassend alle datenschutzrechtlichen Aspekte, die sich im Rahmen von Verarbeitungen ergeben können und findet Anwendung auf sämtliche Arten personenbezogener Daten, insbesondere Daten von Mitarbeiterinnen/Mitarbeitern, Kundinnen/Kunden und anderen Geschäftspartnerinnen/Geschäftspartnern.

Der Geltungsbereich erstreckt sich auf alle Konzernunternehmen und Unternehmensbereiche der STRABAG SE.

Die Herkunft der Daten ist für die Anwendbarkeit dieser Richtlinie nicht maßgeblich. Entscheidend ist die Verarbeitung im Konzern bzw. im Auftrag des Konzerns.

Bestehende gesetzliche Verpflichtungen werden von dieser Richtlinie nicht berührt und sind zu erfüllen. Sofern sich aus gesetzlichen Bestimmungen allerdings geringere Anforderungen ergeben, als die hier dargestellten, gelten die Regelungen dieser Datenschutzrichtlinie.

III. Zulässigkeit der Datenverarbeitung

Bei jedem beabsichtigten Vorgang der Verarbeitung von personenbezogenen Daten ist vorab zu prüfen, ob dieser zulässig ist. Bestehen Zweifel an der Zulässigkeit, sollen die jeweiligen Datenschutzkoordinatorinnen/Datenschutzkoordinatoren kontaktiert werden. Es wird auf Pkt. VI dieser Richtlinie verwiesen.

Es ist zunächst zu prüfen, ob die Datenverarbeitung unter Berücksichtigung des Grundsatzes der Datensparsamkeit überhaupt notwendig ist.

Die weitere Zulässigkeit der Datenverarbeitung kann sich dann aus verschiedenen Gesichtspunkten ergeben.

- Dies ist insbesondere der Fall, wenn die/der Betroffene in die Datenverarbeitung datenschutzkonform eingewilligt hat.

- Auch ohne Einwilligung der/des Betroffenen können Datenverarbeitungen jedoch zulässig sein, wenn eine gesetzliche Ermächtigungsgrundlage (nicht zwingend aus der DS-GVO) gegeben ist. Beispielsweise ist dies der Fall, wenn die konkrete Verarbeitung zur Wahrung der berechtigten Interessen der/des jeweils Verantwortlichen oder einer/eines Dritten erforderlich ist und diese Interessen die entgegenstehenden Interessen der von der Verarbeitung betroffenen Personen überwiegen (Art. 6 Absatz 1 f DS-GVO).
- Ebenfalls zulässig kann die Datenverarbeitung sein, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist (Art. 6 Absatz 1 b DS-GVO).
- Eine Verarbeitung ist auch dann gesetzlich gestattet, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung der/des Verantwortlichen erforderlich ist (Art. 6 Absatz 1 c DS-GVO).
- In Betriebsvereinbarungen oder anderen Kollektivvereinbarungen kann ggf. auch eine Ermächtigungsgrundlage zur Datenverarbeitung gesehen werden. Kollektivvereinbarungen, die als Ermächtigungsgrundlage für eine Datenverarbeitung dienen sollen, sind mit den Datenschutzkoordinatorinnen/Datenschutzkoordinatoren abzustimmen.

Fehlt es an einer Einwilligung und an einer (gesetzlichen) Rechtsgrundlage, dann ist die Datenverarbeitung unzulässig.

Im Rahmen der konzerninternen Datenverarbeitung kann ein berechtigtes Interesse an einer Verarbeitung bestehen, wenn personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, übermittelt werden. In diesen Fällen sind jedoch vorab grundsätzlich die jeweiligen Datenschutzkoordinatorinnen/Datenschutzkoordinatoren einzubinden.

IV. Rechte der Betroffenen

Bei Einführung einer neuen Verarbeitung hat die/der Verantwortliche die von der Verarbeitung Betroffenen über die Umstände der Verarbeitung (z.B. Informationen zur/zum Verantwortlichen, ihren Datenschutzkoordinatorinnen/seinen Datenschutzkoordinatoren, Verarbeitungszweck und Rechtsgrundlage, ggf. Empfängerin/Empfänger der Daten, Speicherdauer) zu informieren.

Über das Auskunftsrecht hat jeder die Möglichkeit, bei der/dem Verantwortlichen Auskunft darüber zu erhalten, inwiefern die/der Verantwortliche personenbezogene Daten der/des Betroffenen verarbeitet. Soweit personenbezogene Daten verarbeitet werden, hat eine Betroffene/ein Betroffener Anspruch auf Auskunft zu den Umständen der Verarbeitung. Die Auskunft ist unverzüglich, also ohne schuldhaftes Zögern, zu erteilen. Im Falle der Verarbeitung unrichtiger Daten besteht ein Anspruch auf Berichtigung.

Bei Vorliegen der gesetzlichen Voraussetzungen haben Betroffene ein Recht auf Löschung der sie betreffenden personenbezogenen Daten (z.B. Wegfall des Verarbeitungszwecks).

Betroffene haben zudem das Recht, die sie betreffenden personenbezogenen Daten, die sie einer/einem Verantwortlichen zur Verfügung gestellt haben, in einem strukturierten, gängigen Format (z.B. PDF-Datei mit OCR-Kennung) zu erhalten und sie einer/einem anderen für die Verarbeitung Verantwortlichen zu übermitteln.

Erfolgt eine Datenverarbeitung durch die Verantwortliche/den Verantwortlichen ohne Einwilligung aufgrund der gesetzesmäßigen Wahrnehmung berechtigter Interessen, so steht der/dem Betroffenen das Recht zu, dieser Verarbeitung zu widersprechen. Grundsätzlich ist einem Widerspruch nur stattzugeben, wenn dieser unter Darlegung persönlicher Versagungsgründe der/des Betroffenen erfolgt, welche die berechtigten Interessen der/des Verantwortlichen überwiegen.

Ein Recht auf Einschränkung der Verarbeitung (nur Speicherung gestattet, jede weitere Verarbeitung nur mit Einwilligung) besteht unter anderem in den Fällen, in denen die Verarbeitung personenbezogener Daten beanstandet wurde, für die Dauer der Klärung. Vor Aufhebung der Einschränkung der Verarbeitung ist die/der Betroffene zu informieren.

Hinsichtlich der Abläufe im Falle der Geltendmachung von Betroffenenrechten wird auf die im DSMS gemachten Ausführungen und Dokumente verwiesen.

V. Verantwortlichkeit

Jede Führungskraft und jede Mitarbeiterin/jeder Mitarbeiter hat dafür Sorge zu tragen, dass die Rechte der/des Einzelnen im Hinblick auf den Datenschutz gewahrt werden.

Die Führungskräfte sind verantwortlich für die Datenverarbeitung in ihrem Verantwortungsbereich. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in dieser Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden. Es ist Aufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen und einen einheitlichen Datenschutzstandard zu etablieren. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiterinnen/Mitarbeiter. Sie handeln für die jeweils Verantwortliche/den jeweils Verantwortlichen und haben dessen Vorgaben zu beachten.
Darauf hinzuweisen ist auch, dass Verstöße gegen die Vorgaben der DS-GVO und

dieser Richtlinie straf-, ordnungswidrigkeits-, haftungs- oder arbeitsrechtliche Konsequenzen nach sich ziehen können.

Im Falle einer Anfrage durch nationale Datenschutzaufsichtsbehörden informieren die Mitarbeiterinnen/Mitarbeiter Ihre zuständige Führungskraft, die wiederum die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren einbezieht. Die Kommunikation mit der Aufsichtsbehörde erfolgt über die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren.

VI. Datenschutzkoordinatorinnen/Datenschutzkoordinatoren

Aufgrund der Bedeutung des Datenschutzes im Konzern wurde zur Umsetzung der erforderlichen Maßnahmen nachstehend näher erläuterte Organisationsstruktur in Form eines Datenschutznetzwerkes geschaffen.

Das Netzwerk der Datenschutzkoordinatorinnen/Datenschutzkoordinatoren setzt sich in den Konzernländern aus je einer Vertreterin/einem Vertreter der CML und des BRVZ zusammen. Die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren wiederum beziehen ihrerseits die operative Ebene – insbesondere durch Kontaktierung der GPM-Beauftragten – ein. Auf Konzernebene erfolgt die zentrale Koordination der Aktivitäten durch eine aus CML und BRVZ IT besetzte Steuerungsgruppe. Diese Datenschutzkoordinatorinnen/Datenschutzkoordinatoren betreuen jeweils alle Fragen und Problemstellungen im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Die aktuelle Liste mit Kontaktdaten der Datenschutzkoordinatorinnen/Datenschutzkoordinatoren ist im STRANET unter der Rubrik „Datenschutz“ abrufbar. Die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren stimmen die datenschutzrechtlichen Aktivitäten der jeweils Verantwortlichen aufeinander ab. Sie sind unter anderem Ansprechpartner für die Betroffenen, die mit der Datenverarbeitung betrauten Mitarbeiterinnen/Mitarbeiter und die Führungskräfte.

Die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren sind auch befugt, die Einhaltung dieser Richtlinie zu prüfen und die Beachtung der gesetzlichen Bestimmungen des Datenschutzrechts zu überwachen. Die entsprechende Überwachungsbefugnis entbindet aber nicht die einzelne Mitarbeiterin/den einzelnen Mitarbeiter von ihrer/seiner Verantwortung. Alle Mitarbeiterinnen/Mitarbeiter haben die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren bei der Erfüllung ihrer Aufgaben und Aktivitäten zu unterstützen.

Bei Bedarf können die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren in Ergänzung zu diesem Datenschutzkonzept Handlungsempfehlungen zu speziellen

Themen herausgeben. Die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren beraten fachlich weisungsunabhängig und überwachen die Einhaltung der Datenschutzvorschriften. Die jeweiligen Konzerngesellschaften und Unternehmensbereiche müssen die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren über neue oder wesentlich veränderte Verarbeitungen personenbezogener Daten informieren. Bei Verarbeitungsvorhaben aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, sind die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren schon vor Beginn der Verarbeitung zu beteiligen. In diesen Fällen haben sie eine Datenschutzfolgeabschätzung vorzunehmen (der Prozess ist im DSMS beschrieben).

Bei Datenschutzverletzungen und Beschwerden sind die Mitarbeiterinnen/Mitarbeiter bzw. die verantwortlichen Führungskräfte verpflichtet, umgehend die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren zu unterrichten. Daneben kann sich jede/jeder Betroffene jederzeit mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes an die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren wenden. Die Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Informationen zu Datenpannen, die personenbezogene Daten betreffen sind den Datenschutzkoordinatoren unverzüglich zur Kenntnis zu bringen. Die als Datenpannen zu verstehenden Sachverhalte sind beispielhaft im DSMS weiter konkretisiert. Die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren prüfen ggf. inwieweit auch eine Informationspflicht gegenüber Aufsichtsbehörden besteht. Eine Information der Aufsichtsbehörden hat innerhalb von 72 Stunden ab Bekanntwerden der Datenpanne zu erfolgen. Die Verantwortlichen arbeiten mit den zuständigen Aufsichtsbehörden kooperativ und vertrauensvoll zusammen. Die Kommunikation mit den Aufsichtsbehörden hat über die Datenschutzkoordinatoren zu erfolgen.

VII. Anforderungen an Mitarbeiterinnen/Mitarbeiter

Eine unbefugte Verarbeitung personenbezogener Daten ist den Mitarbeiterinnen/Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung insbesondere dann, wenn eine Mitarbeiterin/ein Mitarbeiter diese vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das „Need-to-know-Prinzip“: Mitarbeiterinnen/Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten. Mitarbeiterinnen/Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Diese Verpflichtungen bestehen auch nach Beendi-

gung des Beschäftigungsverhältnisses fort.

Alle Mitarbeiterinnen/Mitarbeiter, die personenbezogene Daten verarbeiten, sind tätigkeitsbezogen zu schulen. Entsprechende Schulungen (je nach Erfordernis Präsenzschulungen und/oder E-Learning) werden angeboten.

VIII. Datenschutzkontrolle/Ahndung von Verstößen

Die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren überwachen die Einhaltung der Vorgaben der DS-GVO sowie dieser Richtlinie. Hierzu werden einzelne Bestandteile des DSMS in regelmäßigen Abständen dokumentiert und stichprobenartig überprüft. Es ist daher die Pflicht der/des Einzelnen, die Einhaltung der Vorgaben dieser Richtlinie nachweisen zu können. In Fällen der Feststellung von Verbesserungspotential sind gemeinsam mit den Datenschutzkoordinatorinnen/Datenschutzkoordinatoren Abhilfemaßnahmen festzulegen und in einem Follow-Up-Termin die Umsetzung zu überprüfen.

IX. Meldepflicht von Datenschutzverletzungen

Im Falle der Kenntniserlangung der Mitarbeiterinnen/Mitarbeiter einer Datenpanne, eines Verstoßes gegen diese Richtlinie oder gegen gesetzliche Bestimmungen, die sich auf den Schutz personenbezogener Daten beziehen, sind diese verpflichtet, die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren unverzüglich, d.h. ohne schuldhaftes Zögern, zu informieren. Die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren werden sodann – nach bestätigender Prüfung einer Informationspflicht – unverzüglich eine Meldung an die zuständigen Aufsichtsbehörden sowie die Betroffenen veranlassen.

Die gegebenenfalls erforderliche Kommunikation mit den Aufsichtsbehörden erfolgt über die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren.

Näheres zum Thema wird in der Prozessbeschreibung „Datenpannen“ (hinterlegt im DSMS) geregelt und erläutert.

X. Verzeichnis von Verarbeitungstätigkeiten

Als Verantwortliche haben die konzernangehörigen Gesellschaften ein sogenanntes Verzeichnis von Verarbeitungstätigkeiten zu führen. Dieses Verzeichnis wird entsprechend dem im DSMS vorgegebenen Prozess durch die Datenschutzkoordinatorinnen/Datenschutzkoordinatoren erstellt und gepflegt. Bei jeder Einführung einer

Verarbeitungstätigkeit bezüglich personenbezogener Daten hat eine Information an die regional zuständigen Datenschutzkoordinatorinnen/Datenschutzkoordinatoren verpflichtend zu erfolgen.

XI. Auftragsverarbeitung

Wenn Dienstleister – ganz gleich, ob konzernintern oder konzernextern – im Auftrag einer/eines Verantwortlichen personenbezogene Daten verarbeiten, ist zu beachten, dass die gleichen Sorgfaltsanforderungen wie bei der/dem Verantwortlichen auch für den Dienstleister gelten.

Der Dienstleister wird im Auftrag und unter der Verantwortung der/des Verantwortlichen tätig. Trotz der Durchführung der Datenverarbeitung durch den Dienstleister bleibt der Verantwortliche als solcher Herr der Daten, sodass der Dienstleister sorgfältig auszuwählen ist.

Vor Beginn der Tätigkeit für die/den Verantwortlichen ist dafür Sorge zu tragen, dass der Dienstleister einen gesonderten Vertrag zur Auftragsverarbeitung unterzeichnet hat und die Einhaltung der Pflichten aus dem Vertrag zur Auftragsverarbeitung vorab und sodann regelmäßig kontrolliert werden. Der Auftragsverarbeitungsvertrag ist mit den jeweiligen Datenschutzkoordinatorinnen/Datenschutzkoordinatoren abzustimmen.

Es wird auf die Prozessdefinition „Auftragsverarbeitung“ (hinterlegt im DSMS) verwiesen.

XII. Datensicherheit

Für die jeweils Verantwortlichen ist von großer Bedeutung, dass die Sicherheit der Daten jederzeit gewährleistet ist. Vor diesem Hintergrund sind die Daten unter anderem ausreichend gegen Verlust, gegen unbefugten Zugriff und vor anderen Gefahren zu schützen. Es ist daher dafür Sorge zu tragen, dass angemessene Maßnahmen getroffen werden, um personenbezogene Daten zu schützen. Die technische Planung, Umsetzung und Bereitstellung von Maßnahmen (insbesondere Zentralsysteme und -anwendungen betreffend) ist vorwiegend Aufgabe der BRVZ IT und deren Subunternehmern. Die Umsetzung und Einhaltung im individuellen Arbeitsumfeld liegt in der Verantwortung jeder einzelnen Mitarbeiterin/jedes einzelnen Mitarbeiters. Der Schutz hat durch technische und organisatorische Maßnahmen zu erfolgen (für nähere Erläuterungen verweisen wir auf das DSMS).
Für die einzelnen Vorgänge der Datenverarbeitung sind die konkreten Schutzmaßnahmen zu dokumentieren und auf ihre Angemessenheit hin zu überprüfen. Es kön-

nen weitergehende Vorgaben im Interesse der Datensicherheit durch den Konzern erlassen werden, insbesondere in Bezug auf die Nutzung von IT-Systemen im Konzern.

XIII. Generelles Verbot automatisierter Einzelentscheidungen

Entscheidungen, die für die Betroffene/den Betroffenen negative rechtliche Folgen nach sich ziehen oder sie/ihn erheblich beeinträchtigten können, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung von personenbezogenen Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient, beispielsweise der beruflichen Leistungsfähigkeit. Die Datenverarbeitung darf nur als Hilfsmittel für die Entscheidung herangezogen werden, ohne dabei deren einzige Grundlage zu bilden. Sofern im Einzelfall eine Notwendigkeit für eine automatisierte Einzelentscheidung besteht, muss für die Betroffene/den Betroffenen die Möglichkeit einer Nachprüfung bestehen, wenn nicht eine automatisierte Einzelentscheidung gesetzlich zugelassen ist.

Anhang:

1. Definitionen wesentlicher datenschutzrechtlicher Begriffe

Die nachfolgenden Definitionen entsprechen denen des Art. 4 DS-GVO. Weitere Begriffsdefinitionen finden sich dort.

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „Betroffene/Betroffener“ bzw. „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, 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.

Beispiele: Name, Adresse, Geburtsdatum, IP-Adresse, Foto, biometrische Daten, Personalnummer, Kontoverbindung etc.

„Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

Beispiele: Speichern und Bearbeiten von Daten in einer Cloud, Erfassen von Personen in einem Baustellenzutrittssystem, Arbeiten mit CRM-Tools, Erfassen von Absolventen eines E-Learnings, Arbeiten mit Onlinebewerberplattformen, Bearbeiten von Lohn-und Gehaltsabrechnungen etc.

„Verantwortliche/Verantwortlicher“ ist eine 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. Für den Konzern bedeutet dies, dass jedes Konzernunternehmen für sich jeweils als Verantwortliche/Verantwortlicher im datenschutzrechtlichen Sinne anzusehen ist.

„Auftragsverarbeiterin/Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag der/des Verantwortlichen verarbeitet.

Beispiele: BRVZ für die anderen Konzerngesellschaften, Cloud-Anbieter, Anbieter von Software as a Service-Dienstleistungen (SaaS), auch wenn sie lediglich Daten auf eigenen Servern speichern ohne diese weiter zu verarbeiten, Dienstleister zum Versand der Lohn- und Gehaltsabrechnungen etc.

„Einwilligung“ einer betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

2. Grundsätze der Datenverarbeitung

Die DS-GVO definiert einige Grundsätze, die bei der Verarbeitung von personenbezogenen Daten einzuhalten sind. Jede Mitarbeiterin/jeder Mitarbeiter des Konzerns ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie und damit auch der folgenden Grundsätze verantwortlich. Die Einhaltung ist von ihr/ihm regelmäßig zu kontrollieren.

Es gilt der **Rechtmäßigkeitsgrundsatz**. Damit Verarbeitungen personenbezogener Daten rechtmäßig sind, dürfen diese nur basierend auf einer einschlägigen Rechtsgrundlage oder mit Einwilligung erfolgen.

Der **Zweckbindungsgrundsatz** ist zu beachten. Dies bedeutet, dass die Zwecke einer Verarbeitung vor Beginn derselben abschließend konkret festgelegt werden müssen. Eine anschließende Weiterverarbeitung der einmal erhobenen Daten zu einem anderen Zweck ist nur in Ausnahmefällen gestattet.

Der Grundsatz der **Datenminimierung** ist zu befolgen. Grundsätzlich dürfen daher nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen. Hat sich ein Verarbeitungszweck erledigt, so sind die diesbezüglich gespeicherten Daten zu löschen, es sei denn, gesetzlich ist eine weitergehende Aufbewahrungspflicht (z.B. aus steuerrechtlichen Gründen) vorgegeben.

Zur Wahrung der **Verfügbarkeit, Vertraulichkeit und Integrität der Daten** sowie der Belastbarkeit der datenverarbeitenden Systeme betreibt der Konzern umfangreiche Sicherheitskonzeptionen, die laufend weiterentwickelt werden.

Es gilt der Grundsatz der **Direkterhebung**. Daten sind grundsätzlich bei der/dem Betroffenen direkt zu erheben. Eine Erhebung bei Dritten ist nur dann zulässig, wenn dies gesetzlich vorgesehen ist, sie im Interesse der/des Betroffenen liegt oder eine

Direkterhebung nur mit unverhältnismäßigem Aufwand möglich wäre. Aufgrund des **Transparenzgebotes** ist eine Betroffene/ein Betroffener darüber zu informieren, wenn personenbezogene Daten über sie/ihn verarbeitet werden.

Alle Mitarbeiterinnen/Mitarbeiter haben darauf zu achten, dass personenbezogene Daten **richtig** sind und auf dem neusten Stand gehalten werden. Unzutreffende Daten müssen berichtigt oder gelöscht werden.

Gegenüber betroffenen Personen sollte größtmögliche **Transparenz** im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehen, sodass diese in die Lage versetzt werden, ihre Rechte wahrzunehmen (siehe auch Pkt. IV dieser Richtlinie). Dies setzt voraus, dass alle Informationen und Mitteilungen Verarbeitungen betreffend leicht zugänglich, verständlich und in leicht verständlicher Sprache abgefasst sind.

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss aufgrund des **Accountability**-Grundsatzes zudem jederzeit nachweisbar sein. Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.

Bei der Auswahl neuer Hard- und Software ist das Prinzip der Gewährleistung von **Datenschutz durch Technikgestaltung** und durch **datenschutzfreundliche Voreinstellungen** als tragendes Kriterium zu beachten.