Globale SAP Datenschutz-Policy

Version 3.0, 2019

Inhaltsverzeichnis

Ziel	Die globale SAP-Datenschutz-Policy legt die für den SAP Konzern geltenden Regeln für die Einhaltung des Datenschutzes fest. Die Policy definiert die Grundsätze für den Umgang mit personenbezogenen Daten, bestimmt die Verantwortlichkeiten und Zuständigkeiten innerhalb der Organisation und gibt Hinweise zu deren organisatorischer Umsetzung.
Begründung	
Nutzen	SAP muss bei der Verarbeitung personenbezogener Daten die einschlägigen Gesetze einhalten. Nur so kann SAP die Erwartungen von Behörden, Wirtschaftsprüfern, Datenschutzauditoren, Kunden, Investoren und Geschäftspartnern erfüllen sowie das erforderliche Vertrauen von Mitarbeitern, Bewerbern, Kunden, Lieferanten, anderen Personen und der Öffentlichkeit in den datenschutzkonformen Umgang mit ihren personenbezogenen Daten gewinnen.
Risiko für die SAP bei Nichteinhaltung	Verstöße gegen Datenschutzgesetze können aufsichtsbehördliche Maßnahmen, Bußgelder und auch strafrechtliche Sanktionen nach sich ziehen. Außerdem drohen Unterlassungs- und Schadensersatzforderungen Betroffener. Die Information der Öffentlichkeit über mögliche Verstöße gegen den Datenschutz können die Reputation, die Marke SAP und ihren Wert schädigen.
Geltungsbereich	
Primäre Zielgruppe	Die Policy richtet sich primär an die Unternehmensleitung. Diese hat die Aufgabe, betriebliche Prozesse so zu gestalten, dass die Einhaltung der geltenden Datenschutzgesetze sichergestellt ist.
Indirekt betroffene Bereiche	SAP Mitarbeiter und externe Geschäftspartner, die personenbezogene Daten im Auftrag der SAP verarbeiten, sind verpflichtet, diesen Grundsätzen im Umgang mit personenbezogenen Daten bei ihrer täglichen Arbeit Folge zu leisten.
Geheimhaltungsstufe	Öffentlich.
Durchsetzung	Die Einhaltung der Policy wird mittels der regelmäßigen Beratung durch DPP, die konzernweiten Informationsangebote und Trainings sowie die Verfahrenskontrollen sichergestellt. Die Einhaltung datenschutzrechtlicher Anforderungen wird durch das Datenschutzmanagement System (DPMS) regelmäßig überwacht. Verstöße gegen die Policy werden durch den Bereich DPP unter Hinzuziehung der lokalen Datenschutzkoordinatoren oder sonstiger Funktionen untersucht. Das DPMS selbst wird regelmäßig von externer Seite geprüft und zertifiziert.
Verantwortlichkeiten	
Verantwortliche/r für die Policy	Mathias Cellarius, Konzerndatenschutzbeauftragter der SAP
Vorstandsbereich	Finance and Administration
Verantwortlicher Vorstand	Luka Mucic
Kontaktperson Vorstandsbereich	Mathias Cellarius
Prüfung durch	Scholten, Jochen (Global Legal), Vivianne Gordon-Pullar (Legal Compliance and Integrity Office), Christian Behre (SGS), Alexander Rodde (GRC Internal Controls SE), Barbara Althoff-Simon (Global HR), Rico Modess (Office of CEO), Robin Manherz (IEG).
Genehmigt von	SAP-Vorstand
Dokumentinformationen	
Veröffentlichungsdatum	Version 3.0, 2019

Nächste Prüfung/Aktualisierung	Diese Policy wird alle zwei Jahre bzw. bei wesentlichen Änderungen der Rechtsgrundlagen geprüft.
Versionshistorie	Version 1.0, 2012; Version 2.0, 2017; Version 3.0, 2019

1. Einführung

SAP ist dem Datenschutz verpflichtet. Als solches respektiert und schützt SAP die Rechte des Einzelnen, insbesondere das Recht auf Datenschutz bei der Verarbeitung und Nutzung personenbezogener Daten. Dies gilt für Mitarbeiter, Bewerber, Kunden, Lieferanten, Partner und allen anderen Personen gleichermaßen, deren personenbezogene Daten SAP verarbeitet.

SAP ist ein globales Konzernunternehmen mit Hauptsitz in Deutschland, einem Mitgliedsstaat der Europäischen Union (EU). Konzernmuttergesellschaft ist die SAP SE mit Sitz in Walldorf. Im Vorstand der SAP SE ist das Ressort des Finanzvorstandes für die Einhaltung und Kontrolle des Datenschutzes zuständig. In dessen Auftrag hat der Bereich Data Protection and Privacy (DPP) unter der Leitung des Konzerndatenschutzbeauftragten die globale SAP Datenschutz-Policy ("Policy") erlassen, um der Verpflichtung zum Datenschutz Rechnung zu tragen.

Die Policy legt einen konzerneinheitlichen Standard für einen datenschutzkonformen Umgang mit personenbezogenen Daten fest. Sie definiert Anforderungen für betriebliche Abläufe, die personenbezogene Daten betreffen, und legt klare Verantwortlichkeiten fest. Weitergehende Informationen, themenspezifische Datenschutzstandards und Guidelines können auf der WIKI Seite des Bereichs DPP abgerufen werden.

Die Geschäftsleitung der einzelnen SAP-Konzerngesellschaften und hierunter die zuständigen Prozessverantwortlichen haben sicherzustellen, dass alle Prozesse, bei denen personenbezogene Daten verarbeitet werden, so ausgestaltet sind, dass die Vorschriften dieser Policy erfüllt werden. Als Arbeitgeber tragen SAP-Konzerngesellschaften auch die rechtliche Verantwortung für die Verarbeitung personenbezogener Daten ihrer Beschäftigten. Alle Mitarbeiter haben bei der Handhabung von personenbezogenen Daten im Rahmen ihrer Tätigkeit für SAP die Vorgaben dieser Policy einzuhalten.

Die durch diese Policy aufgestellten Grundsätze beruhen auf der europäischen Datenschutzgesetzgebung und berücksichtigen die Anforderungen der EU Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 - DSGVO). Sie finden grundsätzlich auf alle SAP-Konzerngesellschaften global Anwendung. Im Ausnahmefall kann von ihnen abgewichen werden, wenn

1. anwendbares lokales Recht strengere oder abweichende Datenschutzanforderungen als diese Policy festlegt. In diesem Fall muss die Einhaltung solcher Anforderungen in den lokalen SAP-Konzerngesellschaften sichergestellt werden;

2. im Hinblick auf eine SAP-Konzerngesellschaft der sachliche und räumliche Anwendungsbereich der DSGVO nicht eröffnet ist und das anwendbare lokale Recht geringere Anforderungen als diese Policy stellt. In diesem Fall darf von dieser Policy auf Grundlage einer lokalen Policy unter der Voraussetzung abgewichen werden, dass eine Abweichung keine Auswirkungen auf andere Konzerngesellschaften hat. Abweichungen von dieser Policy sind in jedem Fall mit DPP abzustimmen.

2. Definitionen

Anonyme Daten Anonymisierte Daten	Anonyme bzw. anonymisierte Daten beziehen sich nicht auf eine identifizierbare natürliche Person. Selbst durch Hinzuziehung anderer Daten oder zusätzlicher Informationen ist eine Identifizierung der natürlichen Person nicht bzw. nicht mehr möglich. Die Policy findet auf solche Daten keine Anwendung.
Auftragsverarbeiter	Eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, z. B. ein externer Dienstleister oder eine andere SAP-Konzerngesellschaft, die nicht selbst Verantwortliche Stelle ist.
Besondere Kategorien personenbezogener Daten	Bestimmte personenbezogene Daten, die ihrem Wesen nach besonders sensibel sind, deren Verarbeitung erhebliche Risiken für die Rechte der betroffenen Person verursachen kann und die daher einen besonderen Schutz verdienen. Hierzu zählen Gesundheitsdaten, *genetische* Daten*, biometrischen* Daten zur eindeutigen Identifizierung einer natürlichen Person, Informationen über deren Rasse oder ethnischen Herkunft,

	deren politischen Meinung, religiösen oder philosophischen Überzeugung, der Gewerkschaftszugehörigkeit, des Sexuallebens oder der sexuellen Orientierung. Je nach Kontext können hierzu auch Daten zählen, die zum Zwecke eines Identitätsdiebstahls missbraucht werden können, z. B. Sozialversicherungsnummern, Kreditkarten- und Kontonummern sowie Personalausweis- oder Führerscheinnummern, ferner personenbezogene Daten über strafrechtliche Ermittlungsverfahren, Verurteilungen und Straftaten oder Daten, die unter eine berufsrechtliche Verschwiegenheitspflicht fallen.
Verarbeitung	Verarbeitung bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Die Anonymisierung von Daten stellt ebenfalls eine Verarbeitung von personenbezogenen Daten dar.
Dritter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer • der betroffenen Person, • dem Verantwortlichen • dem Auftragsverarbeiter und • den Personen, die unter der unmittelbaren Verantwortung der Verantwortlichen Stelle oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.
Einwilligung	Jede freiwillige und unmissverständliche Erklärung oder sonstige aktive eindeutig bestätigende Handlung, mit der die betroffene Person in informierter Weise zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten für den bestimmten Zweck einverstanden ist.
Empfänger	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden gelten jedoch nicht als Empfänger, soweit sie personenbezogene Daten im Rahmen eines Untersuchungsauftrages nach dem Unionsrecht oder dem Recht eines EU- Mitgliedstaats erhalten.
Gesundheitsdaten	Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.
Löschen	Die irreversible Unkenntlichmachung oder physische Vernichtung gespeicherter personenbezogener Daten oder deren Anonymisierung auf eine Weise, die es unmöglich macht, die Daten wieder mit der natürlichen Person in Beziehung zu setzen.
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann. Hierzu zählen insbesondere die Zuordnung zu einer Kennung wie einem Namen, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser betroffenen Person sind. Natürliche Personen können beispielsweise direkt aufgrund von Namen, Telefonnummern, E-Mail-Adressen, Postanschriften, Benutzerkennungen, Steuer- oder Sozialversicherungsnummern oder indirekt aufgrund einer Kombination aus beliebigen Informationen identifiziert werden. Personenbezogene Daten, die dieser Policy unterliegen, umfassen insbesondere Daten von Mitarbeitern, Bewerbern, ehemaligen Mitarbeitern, Kunden, Interessenten, Lieferanten, Partnern und Nutzern von SAP Webseiten und -Services. Sie können sich in SAP-eigenen, in Systemen Dritter, die diese

	im Auftrag von SAP betreiben, und ggf. in Kundensysteme befinden, die die Kunden selbst, SAP oder Dritte betreiben, soweit SAP-Mitarbeiter beim Erbringen von Support- oder Beratungsleistungen Zugriff auf darin gespeicherte personenbezogene Daten erlangen können.
Biometrische Daten	Mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu physischen, physiologischen oder verhaltenstypischen Merkmalen einer Person, die eine eindeutige Identifizierung ermöglichen (z.B. Fingerabdrücke oder Gesichtsbilder).
Genetische Daten	Personenbezogene Daten zu ererbten oder erworbenen genetischen Eigenschaften einer Person, die insbesondere aus der Analyse einer biologischen Probe der betreffenden Person gewonnen wurden und eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern.
Pseudonymisierung	Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und dies durch technische oder organisatorische Maßnahmen sichergestellt ist. Pseudonymisierte Daten stellen personenbezogene Daten im Sinne der DSGVO dar, die Policy gilt daher auch für pseudonymisierte Daten.
SAP	SAP SE und ihre weltweiten Niederlassungen und Tochtergesellschaften (verbundene Unternehmen im Sinne von § 15 ff AktG).
DPP	Die bei SAP für das Thema Datenschutz global zuständige Organisationseinheit „Data Protection and Privacy“, die vom Datenschutzbeauftragten der SAP geleitet wird.
DPPC	Auf Ebene der einzelnen SAP Konzerngesellschaften ernannte „Data Protection and Privacy Coordinator“, die die Erreichbarkeit des Konzerndatenschutzbeauftragten sicherstellen und lokal auf die Einhaltung der Policy und des geltenden Datenschutzes hinwirken.
RDPPC	Als regionale Datenschutzkoordinatoren unterstützen die „Regional Data Protection and Privacy Coordinator” die DPPCs bei der Erfüllung ihrer Aufgaben; sie sind dem Konzerndatenschutzbeauftragten unterstellt.
Verantwortliche Stelle	Jede natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Bei SAP ist immer eine SAP- Konzerngesellschaft verantwortliche Stelle für die personenbezogenen Daten ihrer Mitarbeiter, Kunden, Lieferanten, Partner oder anderer Personen. Rein interne Organisationseinheiten oder Gremien wie der Betriebsrat oder gar SAP-Mitarbeiter sind grundsätzlich keine verantwortlichen Stellen. Der Verantwortliche wird durch das rechtlich verantwortliche Management vertreten, z. B. die SAP SE durch die Vorstandsmitglieder oder andere SAP-Konzerngesellschaften durch die Geschäftsführer.

3. Grundsätze des Schutzes von personenbezogenen Daten

Personenbezogene Daten dürfen stets nur im gesetzlich zulässigen Umfang unter Beachtung der nachfolgenden Grundsätze verarbeitet werden.

a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten dürfen nur in rechtmäßiger Weise, unter Beachtung von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies ist der Fall, wenn:

- die Verarbeitung im konkreten Fall gesetzlich erlaubt ist. Gesetzlich erlaubt sind unter anderem alle Fälle der Datenverarbeitung, die

- zur Erfüllung von Verträgen mit der betroffenen Person erforderlich sind (z.B. die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen eines Arbeits- oder Dienstleistungsvertrags),
- im Zuge vorvertraglicher Maßnahmen auf Anfrage des Betroffenen sowie der Vertragsabwicklung mit dem Betroffenen erforderlich sind (z.B. Kunde fordert Informationen zu Produkt X an und erwirbt dieses. Die erforderlichen Daten zur Zusendung des Informationsmaterials sowie zur Abwicklung des Vertragsverhältnisses dürfen verarbeitet werden),
- zur Erfüllung gesetzlicher Pflichten rechtlich erlaubt sind, z.B. aufgrund von Steuer- oder Sozialversicherungsgesetzen,
- zum Schutz lebenswichtiger Interessen einer betroffenen Person erforderlich sind; oder die
- zur Wahrung eines legitimen Interesses der Verantwortlichen Stelle erforderlich sind, welches im konkreten Fall die schutzwürdigen Interessen des Betroffenen überwiegt (z.B. für Direktwerbung);
- auf einer automatisierten Entscheidung im Einzelfall beruht, welche gegenüber der betroffenen Person rechtliche Wirkung entfaltet, wenn diese gesetzliche erlaubt, für die Erfüllung eines Vertrags mit dem Betroffenen erforderlich ist oder die betroffenen Person ausdrücklich eingewilligt hat

oder

- eine betroffene Person ihre Einwilligung dazu gegeben hat (z.B. bei der Registrierung auf einer Website, Anmeldung zu einem Newsletter).

Personenbezogene Daten sollen unmittelbar bei der betroffenen Person erhoben werden. Andernfalls muss die betroffene Person darüber informiert werden, insbesondere welche Arten personenbezogener Daten erhoben, verarbeitet und/oder genutzt werden und zu welchen konkreten Zwecken dies geschieht.

In konkreten Fall sind die Festlegungen zur Zulässigkeit der Verarbeitung und den zu ihrem jeweiligen Schutz erforderlichen technischen und organisatorischen Maßnahmen zu dokumentieren.

b. Zweckbindung

Personenbezogene Daten dürfen nur für eindeutig festgelegte Zwecke erhoben werden. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden.

Der jeweilige Zweck muss vor dem Zeitpunkt der Erhebung festgelegt werden. Eine Verarbeitung zu einem anderen als dem vor der Erhebung festgelegten Zweck ist nur ausnahmsweise zulässig, wenn ein Gesetz die Verarbeitung zu dem anderen Zweck gestattet oder die betroffenen Personen der Verarbeitung zum geänderten Zweck zustimmen. Um festzustellen, ob es sich um vereinbarte Zwecke handelt, sind insbesondere die vernünftigen Erwartungen des Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegenüber dem Unternehmen, die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

c. Datenminimierung

Personenbezogene Daten dürfen stets nur in dem Umfang erhoben werden, der zur Erfüllung des festgelegten Zwecks unbedingt erforderlich ist. Die Verarbeitung hat dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt zu sein.

d. Richtigkeit

Personenbezogene Daten müssen sachlich richtig und aktuell sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich berichtigt, aktualisiert oder gelöscht werden.

Sämtliche Prozesse, die eine Verarbeitung personenbezogener Daten beinhalten, müssen eine Möglichkeit zur Korrektur und Aktualisierung enthalten.

e. Speicherbegrenzung (Pflicht zur Löschung)

Personenbezogene Daten dürfen nur so lange aufbewahrt werden, wie dies für die festgelegten Zwecke bzw. anderen rechtlichen Anforderungen, insbesondere zur Erfüllung gesetzlicher Aufbewahrungsfristen, erforderlich ist. Danach sind personenbezogene Daten grundsätzlich zu löschen oder zu anonymisieren.

Sämtliche Prozesse für die Verarbeitung von personenbezogenen Daten müssen eine Möglichkeit zur Löschung bzw. Sperrung enthalten, soweit dies nach geltendem Recht erforderlich ist.

f. Integrität, Verfügbarkeit und Vertraulichkeit

Personenbezogene Daten und ihre Verarbeitungsvorgänge müssen stets durch technische und organisatorische Maßnahmen angemessen gesichert sein. Dies umfasst insbesondere geeignete Maßnahmen zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Veränderung oder Zerstörung, unbeabsichtigter Offenlegung oder unbefugtem Zugang.

g. Umgang mit besonderen Kategorien personenbezogener Daten

Die Erhebung, Verarbeitung und Nutzung besonderer Kategorien personenbezogener Daten sollen für die betroffenen Personen jederzeit transparent sein. Soweit die Erhebung und Verarbeitung solcher Daten nicht ausdrücklich gesetzlich erlaubt ist, z.B. sofern dies zur Erfüllung von Verpflichtungen im Arbeitsverhältnis, Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist, sollen diese Daten daher nur nach ausdrücklicher vorheriger Information und entsprechender Einwilligung der betroffenen Personen erhoben werden. Die Einwilligungen müssen sich ausdrücklich auf diese besonderen Datenkategorien und deren Verarbeitung für einen oder mehrere festgelegte Zwecke beziehen.

Soweit anwendbares Recht nicht etwas anderes bestimmt, dürfen besondere Kategorien personenbezogener Daten nur mit ausdrücklicher Einwilligung der betroffenen Personen verarbeitet und genutzt werden. Zum Schutz der Daten sind erhöhte Schutzmaßnahmen zu treffen (z.B. physische Sicherheitsvorrichtungen, Zugriffsbeschränkungen und Verschlüsselung).

Prozesse, mittels derer besondere Kategorien personenbezogener Daten erhoben oder genutzt werden, dürfen nur auf Basis einer vorab durchgeführten Datenschutz-Folgenabschätzung und Freigabe durch DPP eingeführt werden.

4. Betroffenenrechte

a. Recht auf Auskunft und Datenübertragbarkeit

Betroffene haben das Recht zu erfahren, ob SAP sie betreffende personenbezogene Daten verarbeitet. In diesem Fall erteilt SAP in dem jeweils rechtlich vorgeschriebenen Maße Auskunft. Die Auskunft wird schriftlich erteilt, es sei denn der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Sie hat sich auf den Zweck der Speicherung, die Empfänger von Daten, sowie alle weiteren gesetzlich geforderten Informationen nach Art. 15 DS-GVO zu erstrecken. Dem Betroffenen ist eine Kopie der personenbezogenen Daten beizufügen, die Gegenstand der Verarbeitung sind.

Auf Anfrage des Betroffenen werden die Daten, die der Betroffene selbst bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt.

b. Recht auf Berichtigung, Einschränkung und Löschung

Erweisen sich personenbezogene Daten als unrichtig, unvollständig oder nicht mehr aktuell, hat jede betroffene Person ein Recht auf Berichtigung ihrer personenbezogenen Daten. Das kann z.B. der Fall sein, wenn eine betroffene Person durch Heirat ihren Namen geändert hat.

Betroffene Personen haben zudem das Recht, die Einschränkung der Verarbeitung ihrer Daten zu verlangen, wenn

- die/der Betroffene die Richtigkeit der Daten bestreitet und die Überprüfung der Richtigkeit eine gewisse Zeit verlangt. In diesem Fall kann die/der Betroffene die Einschränkung für die Dauer der Überprüfung verlangen;
- die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der Daten ablehnt und stattdessen die Einschränkung der Nutzung verlangt;
- die/der Betroffene die personenbezogenen Daten trotz Wegfall des Verarbeitungszwecks und eigentlich bestehender Löschpflicht gleichwohl zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Bei offensichtlicher Kenntnis, dass bestimmte Informationen einen entsprechenden Wert für die betroffene Person haben, muss dem Betroffenen die anstehende Löschung mit angemessener Frist angezeigt werden;
- die betroffene Person gegen die Verarbeitung Widerspruch für die Dauer der Klärung eingelegt hat, ob die berechtigten Gründe für die Verarbeitung gegenüber dem Betroffenen überwiegen.

Im Rahmen der Einschränkung sind die über den Betroffenen gespeicherten personenbezogenen Daten zu markieren, um Zugriffe darauf zu sperren und jede weitere Verarbeitung einzuschränken.

Betroffene Personen haben zudem das Recht auf Löschung personenbezogener Daten, wenn:

- der Zweck der Datenverarbeitung nicht mehr besteht;
- der Betroffene eine erteilte Einwilligung für einen bestimmten Verarbeitungszweck widerruft;
- Adressdaten zu Zwecken des Direktmarketings verwendet werden und der Betroffene hiergegen Widerspruch einlegt;
- die Daten unrechtmäßig verarbeitet werden;
- die Löschung zur Erfüllung rechtlicher Pflichten erforderlich ist.

Alle Prozesse, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, müssen ein Konzept für die regelmäßige Speicherung und Löschung der personenbezogenen Daten aufweisen. Das Konzept hat sicherstellen, dass personenbezogene Daten nach Erfüllung des festgelegten Zwecks oder dem Entfallen der Erlaubnis für die Speicherung, insbesondere gesetzlicher Fristen, rechtzeitig gelöscht werden. Anstelle der Löschung können personenbezogene Daten auch anonymisiert werden.

Besteht eine Pflicht zur Löschung und wurden die personenbezogenen Daten zuvor öffentlich gemacht, sind weitere für die Datenverarbeitung Verantwortliche über das Löschbegehren des Betroffenen hinsichtlich aller Kopien seiner Daten sowie aller Links zu diesen Daten zu informieren.

c. Widerspruchsrecht

Betroffene Personen haben das Recht, einer Datenverarbeitung zu widersprechen, wenn SAP personenbezogene Daten auf Basis einer zu seinen Gunsten ausgehenden Interessenabwägung verarbeitet. In diesem Fall muss die betroffene Person eigene Rechte oder Interessen geltend machen, die das berechtigte Interesse SAPs an der Verarbeitung überwiegen. Der Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung oder eines mit Direktwerbung in Verbindung stehenden Profilings können Betroffene jederzeit und ohne Angabe von Gründen widersprechen.

Im Falle eines Widerspruches wird SAP die Daten für diese Zwecke nicht weiterverarbeiten. Dies gilt nicht, wenn die Verarbeitung aus zwingenden schutzwürdigen Gründen, insbesondere zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen nicht eingestellt werden kann.

d. Beschwerderecht

Sofern eine betroffene Person eine Beschwerde in Bezug auf die Verarbeitung sie betreffender personenbezogener Daten geltend machen möchte, kann sie diese direkt per Email an den Datenschutzbeauftragten schicken: privacy@sap.com.

Der Betroffene ist spätestens innerhalb eines Monats über alle ergriffenen Maßnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.

5. SAP Datenschutz Governance Struktur

Die Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften liegt bei der Geschäftsleitung der jeweiligen SAP-Konzerngesellschaft, die personenbezogene Daten für ihre Geschäftszwecke verarbeitet. Die Geschäftsleitung kann die Aufgabe zur Erfüllung dieser Verantwortung im Rahmen der Organisationsstruktur und der damit verbundenen Geschäftsprozesse an Manager auf unterschiedlichen Ebenen übertragen.

Entsprechend dieser Grundsätze haben die einzelnen globalen SAP Geschäftsbereiche (Line of Business - LoB) den Auftrag zur Umsetzung datenschutzrechtlicher Anforderungen innerhalb ihres Bereichs. Diese Aufgabe von den sogenannten *Management Accountables* der LoBs erfüllt, die die LoB-spezifischen Datenschutz Compliance Maßnahmen festlegen und über ein etabliertes Netzwerk von Koordinatoren und Repräsentanten umsetzen.

Auf der Ebene lokaler SAP Konzerngesellschaften hat die Geschäftsleitung die operative Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften auf den jeweiligen lokalen Finanzverantwortlichen (CFO) zu übertragen. Die CFOs haben für jede SAP Konzerngesellschaft einen Datenschutzkoordinator (DPPC) zu benennen und die erforderlichen Ressourcen für die Umsetzung von Datenschutzmaßnahmen zur Verfügung zu stellen. Lokale Datenschutz Compliance Maßnahmen, die außerhalb der vorbeschriebenen LoB-Struktur erforderlich sind, setzen die CFOs über das so etablierte DPPC Netzwerk um.

Die DPPCs werden zusätzlich von regionalen Datenschutzkoordinatoren (RDPPC) unterstützt. Diese sind dem Konzerndatenschutzbeauftragten unterstellt und berichten somit direkt an DPP. Der RDPPC überprüft die lokalen Datenschutzanforderungen innerhalb der in seiner Verantwortung befindlichen Region und wirkt auf die Umsetzung von Compliance Anforderungen hin. Der RDPPC unterstützt die lokalen DPPCs bei der Erfüllung ihrer Aufgaben und ist Ansprechpartner gegenüber der lokalen Datenschutzaufsicht. Die RDPPCs dürfen keine Anweisungen der lokalen Geschäftsführung erhalten. Sie sind weisungsfrei und dürfen bei der Umsetzung ihrer Aufgaben nicht benachteiligt werden.

Mit diesem Gesamtrahmen zur Steuerung und Überwachung stellt der SAP Konzern die Einhaltung der geltenden Datenschutzanforderungen sicher.

6. Verantwortlichkeiten für die Einhaltung des Datenschutzes

a. Geschäftsführung der SAP Konzerngesellschaften

Die Geschäftsführung einer jeweiligen SAP-Konzerngesellschaft muss sicherstellen, dass die Prozesse in ihrem jeweiligen Verantwortungsbereich, in denen personenbezogene Daten verarbeitet werden (nachfolgend „Prozesse“), die Anforderungen dieser Policy erfüllen. Zu dieser Verantwortung zählen insbesondere folgende Aufgaben:

- Benennung eines DPPC für ihre jeweilige SAP-Konzerngesellschaft und entsprechende Mitteilung an DPP. Die Bestellung eines gemeinsamen DPPCs für mehrere SAP-Konzerngesellschaften ist möglich;
- Ausstattung der DPPCs mit den für die Erfüllung ihrer Aufgabe erforderlichen zeitlichen und sonstigen Mitteln, insbesondere die Teilnahme an erforderliche Fort- und Weiterbildungsmaßnahmen;
- Sicherstellung, dass lokale Prozesse im zentralen Verfahrensregister (PET) eingetragen und regelmäßig auf Aktualität überprüft werden;
- Sicherstellung, dass Prozesse in Einklang mit dieser Policy und anwendbarem Recht stehen;
- Information der lokalen und globalen Prozessverantwortlichen über Änderungen im anwendbaren Recht;
- Sicherstellung, dass in Abstimmung mit dem Konzerndatenschutzbeauftragten erforderliche Meldungen an die örtlichen Aufsichtsbehörden erfolgen und ggf. erforderliche Genehmigungen vorliegen.

b. DPMS Organisation

Seit 2010 wurde bei SAP ein konzernweites Datenschutz Managementsystem (DPMS) implementiert. Es basiert auf der oben beschriebenen Zuweisung der Verantwortung für die Einhaltung des Datenschutzes an die LoBs. Innerhalb einer LoB wird die globale DPMS Organisation durch die Rollen *DPMS Management Accountable*, *DPMS Coordinator* und *DPMS Representative* getragen. Ihre jeweiligen Aufgaben sowie die Funktionsweise des DPMS insgesamt ist im DPMS General Book näher beschrieben. Die SAP-Geschäftsbereiche müssen die erforderlichen personellen, sachlichen und finanziellen Mittel für das DPMS stellen.

Das DPMS selbst wird regelmäßig nach internationalen Standards für Datenschutz Management Systeme auditiert. Das aktuelle Zertifikat kann auf der WIKI Seite von DPP sowie auf der Seite des Cloud Trust Center abgerufen werden.

c. DPPC Organisation

DPPCs wirken in ihrer SAP Konzerngesellschaft auf die Einhaltung der Vorgaben dieser Policy sowie des anwendbaren lokalen Datenschutzrechts hin. Sie haben eine unmittelbare fachliche Berichtslinie an die Geschäftsleitung der SAP-Gesellschaften, für die sie benannt sind, und eine informative Berichtslinie zu DPP. Sie stellen sicher, dass der Konzerndatenschutzbeauftragte aus jeder Konzerngesellschaft heraus leicht erreicht werden kann.

Die Aufgaben der DPPCs ergeben sich aus dem DPPC Handbuch sowie weiterer Handreichungen, die von DPP zur Verfügung gestellt und in Trainings sowie regelmäßigen Abstimmungen vertieft werden. Sie haben ihre Tätigkeiten regelmäßig mit dem DPP abzustimmen, welche auf Basis eines zu Beginn des Jahres festgelegten Umsetzungsplans („Action Plan“) festgelegt werden. Die DPPCs sind von ihren jeweiligen SAP-Konzerngesellschaften bei der Erfüllung ihrer Aufgaben zu unterstützen. Sie sind weisungsfrei in ihrer Aufgabe als DPPC und dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden.

Die Benennung eines neuen DPPC muss von der jeweiligen SAP-Gesellschaft durch den CFO dem DPP rechtzeitig angezeigt werden.

d. Datenschutzbeauftragter und DPP

Der Datenschutzbeauftragte der SAP ist für die gesamte Unternehmensgruppe ernannt. Er ist somit für alle Konzerngesellschaften als Datenschutzbeauftragter zuständig. Der Datenschutzbeauftragte ist in der Ausübung seiner Aufgaben weisungsfrei.

Der Bereich DPP ist dem Datenschutzbeauftragten direkt unterstellt und unterstützt ihn bei der Erfüllung seiner Aufgaben. Die Mitarbeiter des DPP sind nur gegenüber dem Datenschutzbeauftragten weisungsgebunden. Der Datenschutzbeauftragte und die Mitarbeiter des DPP Teams dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden.

DPP definiert die Datenschutzstrategie des SAP-Konzerns im Einklang mit dessen strategischen Zielen und wirkt auf die Einhaltung der geltenden datenschutzrechtlichen Vorschriften in den Konzerngesellschaften hin. Globale und lokale Verantwortliche unterstützen DPP bei der Erfüllung seiner Aufgaben. Insbesondere stellen sie DPP die zur Erfüllung seiner Aufgaben erforderlichen Mittel zur Verfügung und erteilen unverzüglich und vollständig alle erforderlichen Auskünfte.

DPP steuert die DPPCs sowie die RDPPCs und stellt die einheitliche Anwendung datenschutzrechtlicher Vorgaben und ein einheitliches Datenschutzniveau bei SAP sicher. Die RDPPCs werden vom Datenschutzbeauftragten für eine entsprechende Region ernannt und sind Teil von DPP.

Zu den Aufgaben der globalen Organisation siehe Anhang 1.

e. Global Human Resources

Alle SAP Beschäftigten und jede sonst für SAP tätig werdende Person müssen vor Aufnahme einer Tätigkeit für SAP verpflichtet werden, personenbezogene Daten vertraulich zu behandeln und nicht unbefugt zu

erheben, verarbeiten oder zu nutzen (Vertraulichkeit), wenn der Zugang zu personenbezogenen Daten nicht ausgeschlossen werden kann. Dabei ist auf Folgen eines Verstoßes gegen die Verpflichtung hinzuweisen. Ihnen sind diese Policy und andere unternehmensinterne Richtlinien, die den Umgang mit personenbezogenen Daten regeln, zur Kenntnis zu bringen. Die Belehrung muss in schriftlicher oder elektronischer Form dokumentiert werden.

Die Verantwortung für die Verpflichtungen liegt bei SAP Global Human Resources oder im Einzelfall beim verantwortlichen Geschäftsbereich der jeweiligen Konzerngesellschaft.

f. Mitarbeiter

Alle SAP-Mitarbeiter sind verpflichtet, personenbezogene Daten, auf die sie im Rahmen der Erfüllung ihrer Pflichten aus dem Arbeitsverhältnis mit der SAP Zugriff haben, vertraulich zu behandeln und nicht unbefugt zu erheben, verarbeiten oder zu nutzen.

SAP-Mitarbeiter dürfen personenbezogene Daten nur in dem Umfang verarbeiten, der für die Erfüllung ihrer arbeitsvertraglichen Pflichten erforderlich ist. Soweit ein Umgang mit personenbezogenen Daten für den Beschäftigten nicht erkennbar unzulässig ist, kann er sich auf die Rechtmäßigkeit der Anweisungen der Vorgesetzten berufen. Im Zweifel können sich Beschäftigte an die für ihren Bereich zuständigen Datenschutzkoordinatoren oder an DPP wenden (privacy@sap.com). Darüber hinaus stehen jedem Mitarbeiter weitere Informationen auf der DPP WIKI Seite von zur Verfügung.

7. Übermittlung/Auftragsdatenverarbeitung

Sollen personenbezogene Daten innerhalb der SAP-Unternehmensgruppe oder mit anderen Unternehmen ausgetauscht werden, muss zuvor geprüft werden, ob vertragliche Vereinbarungen zu Datenschutz und Datensicherheit erforderlich sind. Eine solche Prüfung ist stets erforderlich, wenn eine SAP Konzerngesellschaft oder ein externer Dienstleister personenbezogene Daten im Auftrag einer (anderen) SAP Konzerngesellschaft verarbeiten soll (sogenannte „Übermittlung zu Verarbeitungszwecken“). Eine Prüfung ist ebenfalls erforderlich, wenn eine SAP Konzerngesellschaft Daten an eine andere SAP Konzerngesellschaft oder an ein externes Unternehmen (z.B. einen Dienstleister, Partner oder Kunden) übermitteln und die empfangende Gesellschaft die Daten für eigene Geschäftszwecke nutzen möchte („Übermittlung für eigene Zwecke“). Die Zulässigkeit der Übermittlung personenbezogener Daten innerhalb der SAP-Gruppe wird mittels eines multilateralen Vertrages, den alle Konzerngesellschaften der SAP Unternehmensgruppe unterzeichnet haben (sog. Intra-Group Data Protection Agreements – IGA) , sichergestellt.

Sollen personenbezogene Daten, die in der rechtlichen Verantwortung einer im europäischen Wirtschaftsraum (EWR) ansässigen SAP-Gesellschaft liegen, in ein Land außerhalb des EWR übermittelt werden, muss zuvor sichergestellt sein, dass ein angemessenes Schutzniveau nach Maßgabe von Art. 44 ff. der Datenschutz-Grundverordnung (EU-Verordnung 2016/79) gewährleistet ist.

Ferner gelten die folgenden Regeln, wenn personenbezogene Daten übermittelt werden:

- **Übermittlung zur Verarbeitung im Auftrag:**

  Beauftragt eine SAP-Konzerngesellschaft eine andere SAP-Konzerngesellschaft oder ein externes Unternehmen mit der Verarbeitung personenbezogener Daten, ist sie für die Einhaltung der datenschutzrechtlichen Anforderungen verantwortlich. Diese Verantwortung erlischt nicht mit der Übergabe der Daten an die andere SAP-Konzerngesellschaft oder das externe Unternehmen.

  Jede SAP-Konzerngesellschaft muss sicherstellen, dass externe Unternehmen, die personenbezogene Daten in ihrem Auftrag verarbeiten sollen, zuvor und sodann regelmäßig auf die Einhaltung der datenschutzrechtlichen Anforderungen überprüft werden und die mit diesen Unternehmen erforderlichen Verträge geschlossen sind. Die Überprüfung kann an zentrale Einheiten innerhalb der SAP-Gruppe delegiert werden. Eine regelmäßige Überprüfung findet ebenfalls innerhalb der Unternehmen der SAP-Gruppe statt.

- **Übermittlung für eigene Zwecke des Empfängers:**

Eine SAP-Konzerngesellschaft darf personenbezogene Daten an eine andere SAP-Konzerngesellschaft oder an ein externes Unternehmen für deren eigenen Zwecke nur dann übermitteln, wenn dies gesetzlich zulässig oder vorgeschrieben ist oder wenn die betroffenen Personen vorher ihre Einwilligung gegeben haben. Die übermittelnde SAP- Konzerngesellschaft muss sicherstellen, dass die rechtlichen Anforderungen vor der Übermittlung geprüft werden.

- **Übermittlung an staatliche Stellen (Behörden und Gerichte):**

  SAP wird personenbezogene Daten an staatliche Behörden und Gerichte nur auf Grundlage geltenden Rechts und nach vorheriger Prüfung durch das DPP sowie Global Legal und unter Einbeziehung anderer erforderlicher Bereiche innerhalb des SAP Konzerns übermitteln.

  Im Falle eines staatlichen Auskunftsgesuchs einer Behörde oder Gerichts wird SAP den Betroffenen hiervon unverzüglich unterrichten.

8. Übermittlung von Kundendaten

SAP verarbeitet personenbezogene Daten von Kunden und im Auftrag von Kunden. Die Nutzung und ggf. Übermittlung solcher Kundendaten muss im Einklang mit den geltenden Gesetzen und vertraglichen Verpflichtungen erfolgen. Personenbezogene Daten von Kunden dürfen ohne eine entsprechende gesetzliche oder vertragliche Grundlage nicht verarbeitet oder an Dritte weitergegeben werden. SAP schließt in allen Fällen datenschutz-relevanter Leistungen mit ihren Kunden entsprechende Auftragsverarbeitungsverträge ab.

SAP arbeitet diesbezüglich mit ihren Kunden zusammen, um sie bei der Einhaltung der geltenden Datenschutzgesetze zu unterstützen; dies beinhaltet jedoch keine Rechtsberatung.

9. Datenschutz-Aufsichtsbehörden

SAP-Konzerngesellschaften müssen stets mit den Datenschutz-Aufsichtsbehörden zusammenarbeiten, sei es aufgrund gesetzlicher Vorschriften, vertraglicher Pflichten oder dieser Policy. Diese Kooperation soll auch grenzüberschreitend erfolgen.

Wenn eine Datenschutz-Aufsichtsbehörde Informationen anfordert oder anderweitig ihr Aufsichtsrecht ausübt, muss DPP unverzüglich informiert werden. Das DPP Team koordiniert die Beantwortung der Anfrage in Abstimmung mit den betroffenen oder anderweitig zuständigen Abteilungen (z.B. Global Legal, Legal Compliance & Integrity, IT Security, Global GRC) und fungiert als direkter Ansprechpartner der jeweiligen Datenschutz -Aufsichtsbehörde.

10. Datenschutz und Sicherheit

Bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko für die betroffenen Personen angemessenes Schutzniveau zu schaffen. SAP definiert solche Maßnahmen im Einklang mit den gesetzlichen Anforderungen in der SAP Security Policy und den daran geknüpften Security Standards und Guidelines. Das DPP Team unterstützt die Definition und Aktualisierung dieser Standards und Guidelines.

11. Schulung

Das DPP Team und die DPPCs führen in regelmäßigen Abständen Schulungen durch. Alle Mitarbeiter und die im Auftrag der SAP tätigen Dritten werden regelmäßig nicht nur über ihre Pflichten, sondern auch über ihre Rechte im Rahmen dieser Policy und der geltenden Gesetze informiert.

12. Externe Zertifizierungen

Zusätzlich zu der genannten Zertifizierung des SAP DMPS nach BS10012:2017 sind viele Bereiche der SAP nach Maßgabe anderer Zertifizierungsstandards zertifiziert. Insbesondere ISO 27001, ISO 9001 etc. Weitergehende Informationen können auf der Cloud Trust Center Webseite abgerufen werden.