Unternehmens-Richtlinien

Prozess Datenschutz Compliance

Datenschutz-Richtlinie

SPB Garant GmbH
SPB Deutschland GmbH

Flößaustraße 22b
D-90763 Fürth

vorgelegt von

atarax Unternehmensgruppe

Luitpold-Maier-Str. 7
D-91074 Herzogenaurach

Bearbeiter:
Schlesinger, Jackwirth

Version 0.2
15.01.2026

Rechtsgebiete
Auch wenn es Überschneidungen mit anderen Rechtsgebieten, wie z. B. Zivil-, Wettbewerbs-, Arbeits- oder Betriebsverfassungsrecht gibt, bitten wir um Ihr Verständnis, dass wir uns aus rechtlichen Gründen auf datenschutzrechtliche Belange beschränken.

Geschlechtsneutrale Formulierung
Ausschließlich zum Zweck der besseren Lesbarkeit wird auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen in diesem Dokument sind somit geschlechtsneutral zu verstehen.

Änderungshistorie

Version	Datum	Bearbeiter	Kapitel	Änderung
0.1	13.11.2020	atarax	Alle	Ersterstellung (E)
0.2	15.01.2026	atarax	Alle	Aktualisierung

1 Vorbemerkung

Der Schutz personenbezogener Daten ist der SPB Garant GmbH, wie auch im selben Maße der SPB Deutschland GmbH (im Folgenden gemeinsam „SPB“) ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden, Lieferanten und aller weiteren Partner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit. Die maßgeblichen Regelungen zum Thema Datenschutz sind in der EU-Datenschutz-Grundverordnung (DS-GVO) sowie in den entsprechenden nationalen Datenschutzgesetzen (in Deutschland im Bundesdatenschutzgesetz, „BDSG“) enthalten. Alle Vorschriften haben das Ziel, die Persönlichkeitsrechte und die Privatsphäre jedes Menschen zu schützen.

2 Datenschutz und Persönlichkeitsrecht

2.1 Leitgedanke und Ziele

Durch diese Richtlinie soll ein einheitlicher Standard für den Schutz personenbezogener Daten bei SPB, vgl. zum Anwendungsbereich Ziffer 2.2., geschaffen werden. Dem erklärten Unternehmensziel, sowohl die Persönlichkeitsrechte der Mitarbeiter als auch der Kunden und weiteren Geschäftspartner zu schützen, soll über ein angemessenes und rechtskonformes Datenschutzniveau entsprochen werden. Die ordnungsgemäße Datenverarbeitung sowie eine wirksame und effektive Datenschutzorganisation sind zentrale Voraussetzungen für die Erfüllung dieses und unserer weiteren Unternehmensziele.

Zudem hat SPB eine so genannte Rechenschaftspflicht. Das bedeutet, dass SPB bei einer etwaigen Datenschutzprüfung die rechtskonforme Datenverarbeitung nachweisen muss. Daher müssen unternehmensweit geltende Richtlinien und die wichtigen Datenschutzprozesse dokumentiert und regelmäßig auf ihre Wirksamkeit geprüft werden.

In Anbetracht der hohen Bußgelder von -je Verstoß- bis zu zwei bzw. vier Prozent des weltweiten jährlichen Jahresumsatzes des gesamten SPB-Konzerns oder 10 bzw. 20 Mio. Euro (der jeweils höhere Betrag gilt) ist dies elementar für unser Unternehmen. Finanzielle Schäden müssen ebenso vermieden werden, wie Imageschäden.

Die Selbstverantwortung des einzelnen Mitarbeiters in seinem jeweiligen Arbeitsbereich und das Erkennen und Bewusstsein, dass ein gelebter Datenschutz ein wesentliches Element unserer Unternehmensphilosophie ist, sind besonders wichtig. Von jedem Mitarbeiter wird ein allzeitiges Bewusstsein um die Bedeutung des Datenschutzes im Arbeitsalltag erwartet.

2.2 Anwendungsbereich

Diese Richtlinie gilt für alle Mitarbeiter unseres Unternehmens, die mit personenbezogenen Daten umgehen. Unternehmen meint

- die SPB Garant GmbH mit allen Betriebsstätten.
- die SPB Deutschland GmbH mit allen Betriebsstätten.

2.3 Verantwortung und Umsetzung

2.3.1 Unternehmensleitung, Führungskräfte, Mitarbeiter

Die **Unternehmensleitung** ist als Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet oder eine Datenverarbeitung im Auftrag vornehmen lässt, „Herr über die Daten“ und insofern für diese verantwortlich. Sie etabliert gesetzeskonformen Datenschutz über ein Datenschutzmanagement einschließlich Instrumenten, Prozessen und Kotrollmechanismen.

Datenschutz ist zudem Bestandteil der originären Führungsaufgabe. Jede **Führungskraft** ist zur Sicherstellung des Datenschutzes in ihrem Aufgabenbereich, also zur Hinwirkung auf die Einhaltung der Vorschriften zum Datenschutz durch ihre Mitarbeiter verpflichtet.

Jeder **Mitarbeiter** trägt durch sein datenschutzbewusstes und an den Maßgaben von Gesetz und unternehmensinternen Vorschriften ausgerichtetes Handeln zum Datenschutz bei. Wer Schwachstellen im Bereich der Datensicherheit oder des Datenschutzes erkennt oder begründet vermutet ist verpflichtet, diese seinem Vorgesetzten oder dem Datenschutzkoordinator bzw. dem Datenschutzbeauftragten unverzüglich und vollständig zu melden.

2.3.2 Datenschutzbeauftragter, Datenschutzkoordinator

SPB hat die atarax Unternehmensgruppe als Datenschutzbeauftragten bestellt. Dieser übernimmt die kraft Gesetzes festgelegten Aufgaben und berät die Unternehmensleitung sowie die Führungskräfte und Mitarbeiter hinsichtlich des Datenschutzes. Der Datenschutzbeauftragte legt mit der Geschäftsleitung das strategische Vorgehen zum Datenschutz fest und unterstützt diese sowie den Datenschutzkoordinator (Ziffer 2.3.3).

Dem Datenschutzbeauftragten obliegt zudem die Kontrolle der Einhaltung der Datenschutzvorschriften im Unternehmen. Er berichtet unmittelbar der Unternehmensleitung. Der Datenschutzbeauftragte ist der Unternehmensleitung direkt unterstellt und agiert gemäß den gesetzlichen Bestimmungen weisungsfrei. Dies ist im Organigramm vermerkt.

Sie können sich zum Thema Datenschutz jederzeit an **info@spb-garant.de** wenden. Unter dieser Adresse erreichen Sie auch den zuständigen Datenschutzkoordinator.

2.3.3 Datenschutzkoordinator

SPB hat außerdem einen Datenschutzkoordinator benannt. Dieser regelt die jeweilige Umsetzung der Datenschutzthemen im Unternehmen und übernimmt die interne Kommunikation vom Datenschutzbeauftragten in das Unternehmen hinein. Er übt insofern die Funktion einer Schnittstelle zwischen Unternehmen und Datenschutzbeauftragtem aus. Sie erreichen Ihn unter info@spb-garant.de.

Grundsätze und Begriffe

2.4 Personenbezogene Daten / Sensible Daten

Von der DS-GVO werden sogenannte „personenbezogene Daten“ geschützt.

Personenbezogene Daten sind alle Informationen, mit denen man die Person identifizieren kann. „Person“ ist dabei nur die natürliche Person, also **jeder Mensch**. Die juristische Person als solche, z. B. die „SPB Deutschland GmbH“, unterliegt nicht dem Anwendungsbereich der DS-GVO. Sobald aber z.B. ein Ansprechpartner oder eine E-Mail-Adresse bestehend aus Vor- und Nachname vorliegt, ist ein Personenbezug gegeben, auch wenn diese Adresse oder dieses Datum allein im geschäftlichen Kontext Verwendung findet.

Für den **Personenbezug** reicht es bereits aus, wenn die Person identifizierbar ist, also anhand anderer Merkmale bestimmt werden kann. Dies gilt auch dann, wenn ein Dritter über die zur Identifikation notwendigen Zusatzdaten verfügt und der Verantwortliche über rechtlich zulässige Mittel verfügt, an diese Informationen zu gelangen. Im Zeitalter der Digitalisierung ist auch an die Identifizierung der Person mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung zu denken.

Beispiele für personenbezogene Daten sind:

- Kontaktdaten (Name, E-Mail-Adresse, Anschrift, Telefonnummer), Familienstand, Geburtsdatum, Beruf, Schulbildung, Fähigkeitsprofil sowie Aussehen
- Daten, die einen Sachverhalt bezeichnen, der mit einer Person verbunden ist, wie z. B. Grundbesitz oder Vermögen

Beispiele für personenbeziehbare Daten sind:

- KFZ-Kennzeichen des Autos
- IMEI-Nummer, IP-Adresse

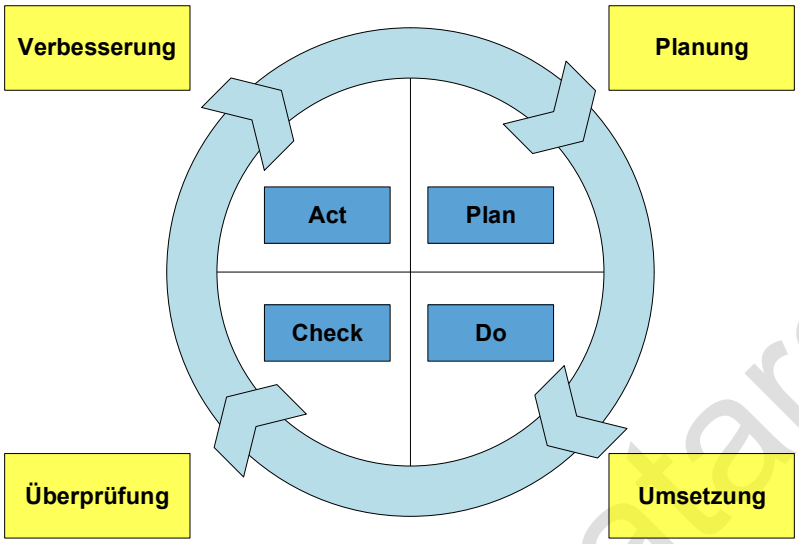
Sämtliche personenbezogenen Daten werden von der DS-GVO geschützt. Art. 9 DS-GVO zählt zudem sogenannte **besondere Kategorien von personenbezogenen Daten** auf. Diese Daten unterliegen aufgrund ihrer besonderen Sensibilität einem **noch strengeren Schutz** und die Verarbeitung ist nur unter restriktiven Vorgaben zulässig. Hierzu zählen:

- Rassische und ethnische Herkunft
- Politische Meinung
- Religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- Gesundheitsdaten
- Genetische und biometrische Daten
- Daten zum Sexualleben oder der sexuellen Orientierung.

2.5 Rechenschaftspflicht

SPB trifft nach Art. 5 DS-GVO eine Rechenschaftspflicht. Dies bedeutet, dass SPB. bei etwaigen Prüfungen durch eine Datenschutzaufsichtsbehörde verpflichtet ist nachzuweisen, dass die im Folgenden näher erläuterten Grundsätze bei der Datenverarbeitung beachtet werden. Weil die Beweislast dafür, keinen Datenschutzverstoß begangen oder diesem angemessen begegnet/ vorgebeugt zu haben damit beim Unternehmen und nicht bei der

staatlichen Stelle liegt, spricht man von einer „umgekehrten Beweislast“. Aufgrund der Nachweispflicht ist ein wirksames und nachweisbares Datenschutzmanagement für die Unternehmensverteidigung elementar.



2.6 Rechtmäßigkeit der Verarbeitung

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte der betroffenen Personen gewahrt werden. Daher müssen die Daten auf rechtmäßige Weise, nach Treu und Glauben und für die betroffene Person nachvollziehbar, also transparent, verarbeitet werden. Die Verarbeitung bzw. eine Datenübermittlung darf nur im Rahmen des rechtlich Zulässigen erfolgen. Jede Datenverarbeitung muss durch eine Rechtsgrundlage legitimiert sein (sogenanntes Verbot mit Erlaubnisvorbehalt – keine Datenverarbeitung ohne Erlaubnis) und kann insofern nach Art. 6 Abs. 1 DS-GVO grundsätzlich rechtmäßig erfolgen:

- für eine vertragliche Beziehung
- zur Erfüllung einer rechtlichen Verpflichtung / Wahrnehmung von öffentlichen Aufgaben
- zum Schutz lebenswichtiger Interessen
- aufgrund einer Einwilligung
- zur Wahrung berechtigter, im Rahmen einer Abwägung überwiegender Interessen

Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten von z.B. Interessenten, Kunden oder anderen Geschäftspartnern dürfen zur Durchführung der vorvertraglichen Maßnahmen, zur Vertragsdurchführung und zur Beendigung des Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. In der Vertragsanbahnungsphase ist die Verarbeitung der Daten für z. B. Angebote etc. erlaubt.

Entsprechend dürfen Mitarbeiter- (bzw. Bewerber-) Daten verarbeitet werden, wenn diese für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses erforderlich sind. So muss der Arbeitgeber z. B. zur Überweisung des Gehalts Ihre Kontodaten wissen.

Wenn die für Verträge erhobenen Daten allerdings zu Werbe- oder sonstigen anderen Zwecken genutzt werden sollen als zu denen, für deren Verfolgung sie ursprünglich erhoben wurden, sind die diesbezüglichen besonderen Voraussetzungen zu beachten. Hier ist es

wichtig, dass Sie ggfs. unsere internen Bereichs-/ Vorgangs-spezifischen Vorgaben beachten und ggf. Rücksprache mit dem Fachverantwortlichen oder dem Datenschutzkoordinator halten.

Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung / Wahrnehmung von öffentlichen Aufgaben

Personenbezogene Daten dürfen verarbeitet werden, wenn eine rechtliche Verpflichtung dazu besteht bzw. eine staatliche Rechtsvorschrift die Datenverarbeitung erfordert oder gestattet (z. B. Meldungen von Daten an das Finanzamt / Sozialversicherungsträger). Gleiches gilt, wenn die Verarbeitung zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Dieses Interesse muss sich immer aus einer Rechtsvorschrift ergeben.

Datenverarbeitung zum Schutz lebenswichtiger Interessen

Personenbezogene Daten dürfen zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person verarbeitet werden. Wenn ein Mitarbeiter z. B. umgehend medizinische Hilfe benötigt, dürfen dem Rettungsdienst die erforderlichen Angaben über den Mitarbeiter gemacht werden, insbesondere relevante Gesundheitsdaten.

Datenverarbeitung aufgrund von Einwilligungen

Die Datenverarbeitung kann auch mit Einwilligung der betroffenen Person erfolgen (z.B. Werbeeinwilligung). Jede Einwilligung muss freiwillig, aktiv und informiert erteilt werden. Ferner muss die Einwilligung den Vorgaben des Art. 7 DS-GVO entsprechen, andernfalls ist sie unwirksam. Muster für Einwilligungen sind vor Verwendung mit dem Datenschutzbeauftragten abzustimmen. Jede erforderliche Einwilligung muss zudem zum Nachweis schriftlich oder elektronisch dokumentiert werden.

In Bezug auf Einwilligungen im Arbeitsverhältnis und von Minderjährigen bestehen Spezialregelungen, die unbedingt beachtet werden müssen.

Datenverarbeitung zur Wahrung berechtigter Interessen

Personenbezogene Daten dürfen verarbeitet werden, wenn dies zur Wahrung der berechtigten Interessen SPB erforderlich ist und keine schutzwürdigen Interessen Betroffener überwiegen. Eine umfassende, dokumentierte Interessenabwägung ist vorzunehmen. Berechtigte Interessen des Unternehmens, die entgegenstehenden Betroffeneninteressen überwiegen, sind regelmäßig rechtliche oder wirtschaftliche Interessen (z. B. Durchsetzung von Forderungen, Vermeidung von Vertragsstörungen).

Könnten aber schutzwürdige Interessen der betroffenen Person das berechtigte Interesse an der Verarbeitung überwiegen, darf eine Verarbeitung nicht erfolgen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen und zu dokumentieren.

Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger Daten darf nur erfolgen, wenn dies gesetzlich zulässig ist oder die betroffene Person ausdrücklich und freiwillig eingewilligt hat. Die Verarbeitung ist z. B. zulässig, damit der Verantwortliche oder die betroffene Person Pflichten aus dem Arbeits- und Sozialrecht bzw. hieraus erwachsenen Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann oder wenn die Verarbeitung der Daten zwingend notwendig ist, um rechtliche Ansprüche gegenüber der betroffenen Person geltend zu machen oder zu verteidigen.

2.7 Datenminimierung

Jede Verarbeitung personenbezogener Daten muss so angelegt sein, dass möglichst wenige Daten verarbeitet werden. Es dürfen also **in jedem Fall nur die Daten verarbeitet werden, die objektiv zwingend für die Aufgabenerfüllung bzw. den verfolgten Zweck erforderlich sind**. Bei IT-Systemen sind zudem Pseudonymisierung und Anonymisierung (Ausschluss der Rückverfolgbarkeit) zu prüfen. Auf anonyme Daten findet die DS-GVO schließlich keine Anwendung.

Ein Praxisbeispiel für die Umsetzung des Grundsatzes der Datenminimierung sind Kontaktformulare. Hier muss bei der Angabe der Kontaktdaten zwischen freiwilligen und verpflichtenden Feldern unterschieden werden. Letztere sind für die Durchführung der Kontaktanfrage erforderlich und dürfen daher auch verpflichtend abgefragt werden. Alle übrigen Angaben müssen aber als freiwillig gekennzeichnet werden. Eine verpflichtende Erhebung auch solcher Daten, die nicht zwingend zur Bearbeitung der Kontaktanfrage erforderlich sind, wäre ein Verstoß gegen die DS-GVO und damit bußgeldbewehrt.

2.8 Zweckbindung der Datenverarbeitung

Vor der Verarbeitung der personenbezogenen Daten muss ein legitimer Verwendungszweck festgelegt und in das Verzeichnis der Verarbeitungstätigkeiten (VVT) aufgenommen werden. Die zweckgebundene Verarbeitung ist nachweislich sicherzustellen. Nachträgliche Zweckänderungen sind unter engen Voraussetzungen möglich und müssen dokumentiert werden.

2.9 Datenqualität

Die verarbeiteten Daten müssen sachlich richtig und aktuell sein. Es müssen alle angemessenen Maßnahmen getroffen werden, damit personenbezogene Daten im Hinblick auf den Verarbeitungszweck berichtigt werden.

2.10 Speicherbegrenzung

Personenbezogene Daten sind zu löschen, sobald der definierte Zweck für die Datenverarbeitung entfallen ist. Diese Anforderung kann im Spannungsverhältnis zu rechtlichen Aufbewahrungspflichten stehen. Vereinfacht gilt:

- Personenbezogene Daten sind zu löschen, sobald diese nicht mehr benötigt werden,
- es keine gesetzliche Aufbewahrungspflicht mehr gibt und
- keine rechtlichen Aufbewahrungsgründe (z.B. zur Erfüllung von Rentenansprüchen, zur Abwehr zivilrechtlicher Klagen etc.) mehr bestehen.

SPB etabliert zur Erfüllung dieser rechtlichen Anforderung ein individuelles und bedarfsgerechtes Löschmanagementsystem, angelehnt an die DIN66398.

2.11 Datensicherheit / Vertraulichkeit

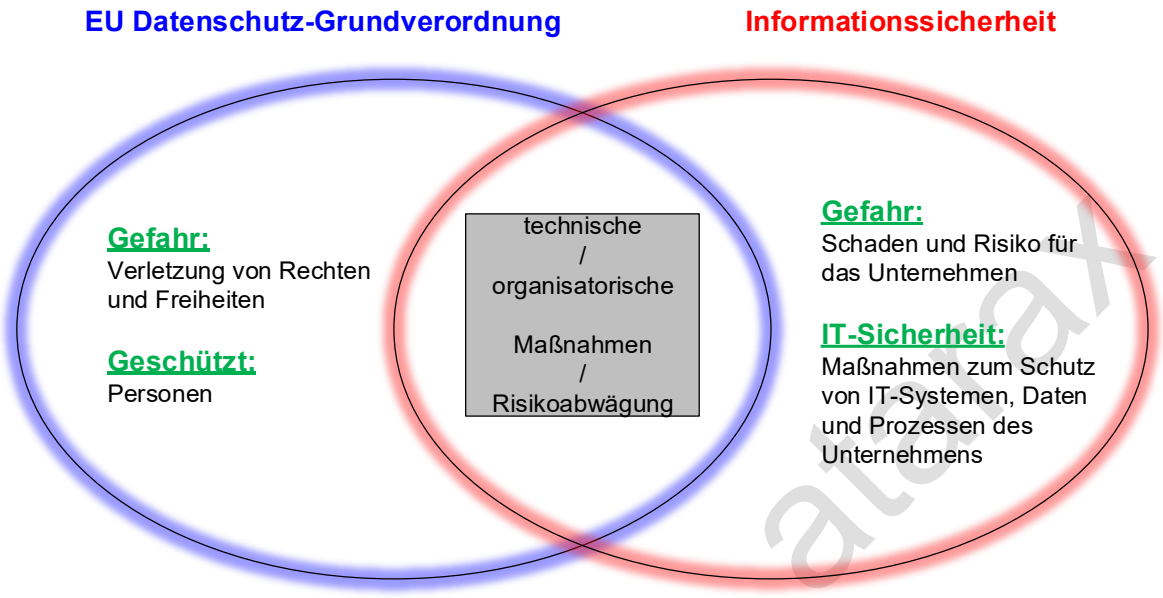


Abbildung: Gemeinsamkeiten von Datenschutz und IT-Sicherheit.

Personenbezogene Daten müssen so verarbeitet werden, dass eine angemessene Datensicherheit gewährleistet wird. Die Daten müssen jederzeit gegen unbefugten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Zerstörung oder Schädigung geschützt werden. Dies hat durch geeignete technische und organisatorische Maßnahmen zu erfolgen und gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt.

Die Sicherheitsmaßnahmen müssen also die Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten als auch die Belastbarkeit der Systeme sicherstellen.

Sicherheitsmaßnahmen sind risikoorientiert und unter Berücksichtigung des Standes der Technik sowie der Implementierungskosten zu treffen. Risikoanalysen aus Sicht des Betroffenen sind für die Datenverarbeitungsprozesse durch die Fachabteilung in Zusammenarbeit mit der IT durchzuführen und müssen dokumentiert werden. Hierbei werden die Art, der Umfang, die Umstände sowie der Zweck der Verarbeitung als auch die Eintrittswahrscheinlichkeit einer Gefahr sowie die Auswirkung eines (möglichen) Schadens berücksichtigt.

Zu den erforderlichen Maßnahmen gehören gem. der DS-GVO auch Maßnahmen zur Pseudonymisierung sowie Verschlüsselung der Daten. Wenn besonders sensible Daten, wie z. B. Gesundheitsdaten, aber auch Bewerberdaten an SPB übermittelt werden sollen, müssen diese zum Schutz vor „Angreifern“ verschlüsselt bzw. jedenfalls eine Verschlüsselungsoption angeboten werden. Zudem muss SPB ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen nachweisen können.

Datensicherheit kann nur garantiert werden, wenn alle Mitarbeiter mit den Daten sorgsam umgehen und diese vertraulich und im Rahmen ihrer Befugnisse behandeln. Es gilt das so genannte Need-to-know-Prinzip, d.h. jeder Mitarbeiter darf nur Zugang zu den

personenbezogenen Daten erhalten, soweit dies für die jeweilige Aufgabenerfüllung erforderlich ist, er also ein objektives Wissensbedürfnis hat.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Insofern sollen alle Mitarbeiter im Regelfall bei Arbeitsaufnahme eine entsprechende Verpflichtungserklärung unterschreiben.

Jeder Mitarbeiter muss die personenbezogenen Daten in seinem Verantwortungsbereich ausreichend gegen unberechtigten Zugriff bzw. Verarbeitung sowie Verlust schützen und verfügbare Lösungen nutzen (z. B. Passwortsperre, Wegschließen von vertraulichen Unterlagen, datenschutzkonforme Vernichtung / Shreddern, aufgeräumter Schreibtisch, Verschlüsselung von E-Mails, sicheres Format beim Versenden, z.B. PDF).

3 Datenschutz-Prozesse

3.1 Rechte der betroffenen Personen

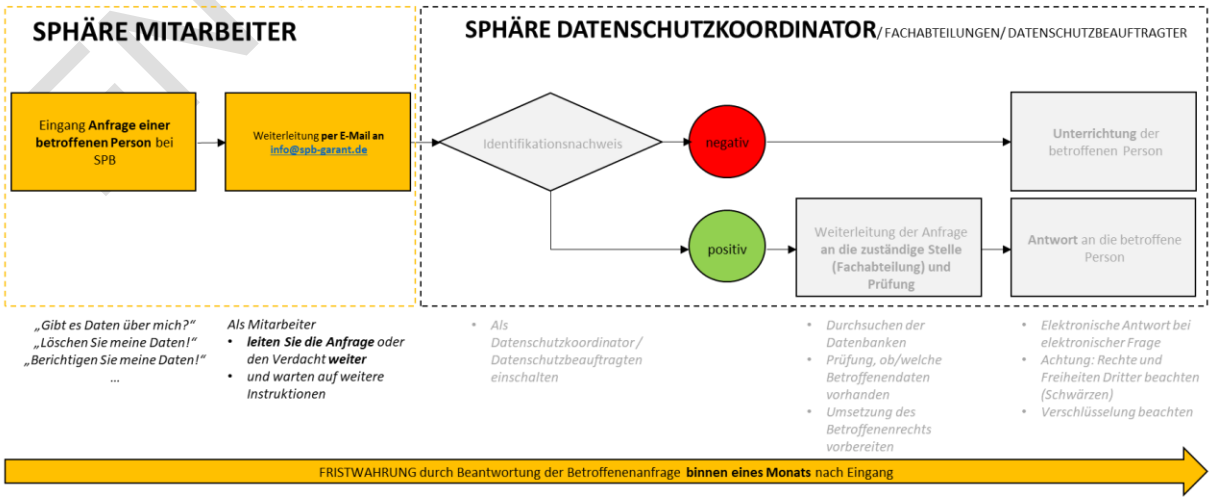
Die betroffenen Personen, von denen SPB personenbezogene Daten verarbeitet (z.B. Kunde, Lieferant, andere Geschäftspartner, aber auch eigene Mitarbeiter) haben als so genannte „Betroffene“ Rechte. Jeder Mitarbeiter ist verpflichtet, sich mit diesen Rechten und den Prozessabläufen vertraut zu machen und danach zu handeln. Die Mitarbeiter werden zudem in regelmäßigen Schulungen dazu sensibilisiert. Auch werden die Prozesse regelmäßig in Tests („Feuerwehrübungen“) geprüft und hinsichtlich Effektivität und Korrektheit kontrolliert. Mit Ausnahme des Betroffenenrechts zur Beschwerde über eine Datenverarbeitung bei der Datenschutz-Aufsichtsbehörde ist regelmäßig das Unternehmen als für die Datenverarbeitung verantwortliche Stelle Adressat von Betroffenenanfragen.

Diese Betroffenenrechte sind gesetzlich vorgesehen und können auf jedem Weg bei SPB geltend gemacht werden:

- Auskunft
- Berichtigung
- Löschung
- Datenübertragung
- Widerspruch
- Widerruf
- Einschränkung der Verarbeitung
- Nicht einer vollständig automatisierten Entscheidung unterworfen zu werden

Betroffenenanfragen oder Zweifelsfälle müssen unverzüglich und vollständig an info@spb-garant.de gemeldet werden.

Der **Bearbeitungsprozess** für jegliche Betroffenenfragen orientiert sich grundsätzlich an folgendem Muster:



3.1.1 Auskunft, Art. 15 DS-GVO

Das Auskunftsrecht des Betroffenen umfasst das Recht darauf,

- Bestätigung darüber zu verlangen, ob personenbezogene Daten über sie verarbeitet werden,
- ggfs. Auskunft über diese personenbezogenen Daten zu beanspruchen,
- eine unentgeltliche Kopie der personenbezogenen Daten zu erhalten.

Wenn Persönlichkeitsrechte anderer Personen entgegenstehen, darf keine Kopie herausgegeben werden oder diese Inhalte müssen unkenntlich gemacht werden.

3.1.2 Berichtigung, Art. 16 DS-GVO

Das Recht auf Berichtigung umfasst die folgenden Anspruchsinhalte zu Gunsten des Betroffenen:

- Unverzügliche Berichtigung der ihn betreffenden unrichtigen personenbezogenen Daten (z.B., weil sich die Adresse geändert hat).
- Je nach Verarbeitungszweck Vervollständigung personenbezogener Daten.
- Bei erfolgter Offenlegung an andere Stellen (z. B. Dienstleister) Information aller Empfänger über Datenberichtigung (außer unmöglich oder unverhältnismäßig).

3.1.3 Löschung („Recht auf Vergessenwerden“), Art. 17 DS-GVO

Das Recht auf Vergessenwerden (Löschung) hat zum Gegenstand:

- Unverzügliche Löschung, wenn die Daten für den Verarbeitungszweck nicht mehr erforderlich sind, eine Einwilligung widerrufen oder ein Widerspruch eingelegt wurde und keine Aufbewahrungspflichten der Löschung entgegenstehen.
- Verpflichtung des Verantwortlichen zur Information etwaiger Datenempfänger über den Löschanspruch.

3.1.4 Einschränkung der Verarbeitung, Art. 18 DS-GVO

- Voraussetzungen: Richtigkeit der Daten streitig, Verarbeitung der personenbezogenen Daten unrechtmäßig oder Geltendmachung, Ausübung oder Verteidigung von rechtlichen Ansprüchen gegenständlich.
- Folge: Daten dürfen -von Speicherung abgesehen- nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte anderer natürlicher oder juristischer Personen bzw. aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden. Hierüber müssen etwaige Empfänger dieser Daten informiert werden.

3.1.5 Datenübertragung, Art. 20 DS-GVO

Das Wesen des Rechts auf Datenübertragbarkeit umfasst folgende Aspekte:

- Anspruch des Betroffenen, die ihn betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.
- Erstreckung nur auf Daten, die der Betroffene selbst zur Verfügung gestellt hat, und die automatisiert auf Basis eines Vertrags oder einer Einwilligung verarbeitet wurden.
- Recht auf Datenübertragbarkeit besteht nicht, wenn Rechte und Freiheiten anderer Personen betroffen sind.
- Die rechtmäßig beanspruchte Datenübertragung muss gratis erfolgen.

3.1.6 Widerspruch, Art. 21 DS-GVO

Das Recht auf Widerspruch gegen eine Datenverarbeitung bedeutet:

- Eine Möglichkeit, gegen die Datenverarbeitung aus Gründen, die sich aus der besonderen Situation des Betroffenen ergeben, vorzugehen, wenn die Verarbeitung aufgrund einer vorausgehenden Interessenabwägung stattfindet.
- Keine weitere Verarbeitung, außer die SPB kann zwingende schutzwürdige Gründe für die Weiterverarbeitung nachweisen welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.
- Eine zwingende Interessenabwägung, die immer Einzelfallabwägung ist.
- Zudem: Die Möglichkeit eines Widerspruchs gegen eine Datenverarbeitung für Direktwerbung oder Profiling.

3.1.7 Widerruf von Einwilligungen, Art. 7,8 DS-GVO

Macht der Betroffene rechtmäßig von seinem Recht auf Widerruf einer Einwilligung Gebrauch, greift diese Widerrufsfolge: Die betreffende Datenverarbeitung darf nicht mehr stattfinden, wenn die Einwilligung die Rechtsgrundlage für die betreffende Datenverarbeitung war. Der Widerruf ist unverzüglich umzusetzen; dies ist systemseitig entsprechend abzubilden (z.B. im CRM-System, Newsletter-Tool, …). Jeder Widerruf einer Einwilligung muss so einfach möglich sein wie die Erteilung der Einwilligung selbst es war.

Die DS-GVO schreibt vor, Betroffene umfassend über die Datenverarbeitung im Unternehmen zu informieren. Dies betrifft nicht nur Kunden und Interessenten, sondern gilt auch gegenüber unseren Mitarbeitern, da auch diese im Rechtssinne Betroffene sind.

Wichtig ist, dass bei der Implementierung der Pflichtinformationen bedacht wird, sämtliche Szenarien und ‚Kontaktpunkte' mit allen Gruppen betroffener Personen (s.o. Kunden, Interessenten, Mitarbeiter) zu berücksichtigen, damit sowohl im Online- (z.B. Webseite, Webshop) als auch im Offline-Bereich (stationärer Vertrieb, Messekontakte, etc.) und bei telefonischen Kontakten, die Datenerhebungen bei Betroffenen mit sich bringen, Transparenzanforderungen eingehalten werden können.

Was Inhalt, Form und Zeitpunkt der Information angeht, so ergeben sich die Anforderungen an die Betroffeneninformation direkt aus den Artikeln 13 und 14 DS-GVO. Aus diesem Grund sind Betroffeneninformationen stets individuell zu erstellen und müssen auf den Kanal ihrer Verbreitung zugeschnitten sein (z.B. Papiere, Website, Apps, Social Media, …).

3.2 (Keine) automatisierte Entscheidung im Einzelfall einschließlich Profiling

Nach Art. 22 Abs. 1 DS-GVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt (sogenanntes Profiling, z.B. Scoring).

Automatisierte Entscheidungen sind jedoch zulässig, wenn dies für den Abschluss oder die Erfüllung eines Vertrags nötig ist oder mit ausdrücklicher Einwilligung der betroffenen Person erfolgt oder bereits aufgrund von Rechtsvorschriften zulässig ist. Bei Einwilligungen ist grundsätzlich Vorsicht geboten, da die DS-GVO diese Rechtsgrundlage anerkennt, jedoch in Art. 7 Abs. 4 DS-GVO betont wird, dass die Einwilligung freiwillig erfolgen muss (sogenanntes Kopplungsverbot).

Art. 22 Abs. 3 DS-GVO verlangt, dass wir als Unternehmen angemessene Maßnahmen zum Schutz der Rechte und Freiheiten Betroffener treffen. Dazu zählt mindestens das Recht der Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, das Recht auf Darlegung des eigenen Standpunkts und auf Anfechtung der seitens des Verantwortlichen getroffenen Entscheidung. Dieses sogenannte Remonstrationsrecht bedingt, dass wir als Unternehmen entsprechende Anfragen Betroffener bearbeiten müssen.

Darüber hinaus dürfen laut Art. 22 Abs. 4 DS-GVO Entscheidungen nach Absatz 2 grundsätzlich nicht auf besonderen Kategorien personenbezogener Daten beruhen; eine Ausnahme gilt bei Einwilligungen.

3.3 Meldepflicht bei Datenpannen

Wird der Schutz personenbezogener Daten verletzt, müssen wir dies an die zuständige Datenschutzaufsichtsbehörde melden. Die Meldepflicht besteht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten Betroffener führt. **Die Meldung muss binnen 72 Stunden erfolgen**. Daher müssen interne Melde- und Eskalationswege eingehalten werden, um etwaigen Pannen sofort zu begegnen.

Die **interne Meldeadresse** lautet **info@spb-garant.de** .

Nehmen Sie nie eigenmächtig eine Meldung an die Aufsichtsbehörde vor!

3.4 Outsourcing / Verträge über Auftragsverarbeitung

Bei der Zusammenarbeit mit Dienstleistern, die in unserem Auftrag und auf unsere Weisung hin unsere personenbezogenen (Kunden-/Mitarbeiter/Online-) Daten verarbeiten, bedarf es einer datenschutzrechtlichen Vereinbarung, eines sogenannten Auftragsverarbeitungs-Vertrags, der vor Beginn der Zusammenarbeit geschlossen werden muss.

Eine sorgfältige Dienstleisterauswahl muss nachgewiesen werden, da Auftragsverarbeiter als datenverarbeitende Stelle mit einer Vielzahl personenbezogener (Kunden- und Mitarbeiter-) Daten umgehen. Das bedingt, dass wir als Auftraggeber sicherzustellen haben, dass geltende Datenschutzstandards eingehalten werden. Dies meint vor allem gesetzliche Vorgaben, aber auch weitere vertragliche oder sektor- bzw. branchenspezifische Vorgaben.

Ergänzend müssen Auftragnehmer in regelmäßigen Abständen geprüft werden. Es muss daher stets nachvollziehbar sein, mit welchen Dienstleistern zusammengearbeitet wird und dass die erforderlichen Datenschutzverträge in aktueller Gestalt existieren.

Besonderheiten ergeben sich bei Rechtsgrundlagen der Datenübermittlung in sogenannte Drittstaaten, die außerhalb der EU bzw. des EWR liegen. Dies betrifft z.B., aber nicht nur Dienstleister in den USA. Aufgrund der Komplexität muss das Thema Datentransfers ins Ausland stets gesondert geprüft werden.

3.5 Verarbeitungsübersicht

Diese Dokumentation aller Vorgänge der Verarbeitung personenbezogener Daten durch SPB als Verantwortliche Stelle und durch unsere Auftragsverarbeiter hat wegen der Rechenschaftspflicht besonderes Gewicht: Sie ist ein zentrales Dokument zum Nachweis der Rechtskonformität. An Art. 30 DS-GVO, der die Pflichtinhalte nennt, orientierte Interne Vorlagen stehen zur Verfügung.

Diese enthalten auch Angaben zu Rechtsgrundlagen der betreffenden Datenverarbeitung und eine diesbezügliche Risikobewertung. Dadurch können die Rechtmäßigkeit der Datenverarbeitung und die damit verbundenen Risiken für Betroffene dokumentiert werden, was als Basis für weitere Aspekte des Datenschutzmanagements dienen kann.

Die DS-GVO verlangt in Art 30 II zudem, dass jeder Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führt. Im Fall von Auftragsverarbeitung für andere müssen wir demnach ein entsprechendes Dokument erstellen.

3.6 Datenschutz-Folgenabschätzung

Für risikobehaftete Verarbeitungen ist eine Datenschutz-Folgenabschätzung durchzuführen. Wird ein solches Verfahren eingeführt oder geändert, ist eine entsprechende Prüfung durchzuführen und zu dokumentieren. Besonderes Augenmerk ist auf die Risikoeinschätzung zu legen.

Die DS-GVO sieht vor, dass die Aufsichtsbehörden einen Katalog erstellen, der Konstellationen benennt, in denen eine Datenschutz-Folgenabschätzung durchzuführen ist. Dies bedeutet, dass in bestimmten Fällen ungeachtet des Bestehens eines hohen Risikos für die Rechte und Freiheiten Betroffener keine zwingende Datenschutz-Folgenabschätzung oder aber die Abschätzung gerade zwingend durchzuführen ist.

Wenn die Bewertung im Rahmen einer Datenschutz-Folgenabschätzung ergibt, dass trotz (ggfs. ergänzender) Schutzmaßnahmen ein Restrisiko für die Rechte und Freiheiten Betroffener durch die Datenverarbeitung bleibt, ist die Datenschutzaufsicht zu konsultieren.

3.7 Datenschutzkontrollen

Die Einhaltung der Maßgaben zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch eigene dokumentierte Datenschutzprüfungen validiert. Zudem kann die zuständige Datenschutzaufsichtsbehörde im Rahmen der ihr nach anwendbarem Recht zustehenden Befugnisse auch ihrerseits Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen. Solche Kontrollen können ebenso auf Grund situativer Veranlassung, wie auch anlassunabhängig erfolgen.

3.8 Definition und ständige Verbesserung der technischen und organisatorischen Maßnahmen

Personenbezogene Daten sind durch angemessene technische und organisatorische Maßnahmen zu schützen und nach Möglichkeit zu anonymisieren oder zu

pseudonymisieren. Risiko der Verarbeitung und Stand der Technik sind zu berücksichtigen. Datenschutzmanagement und Informationssicherheitsmanagement müssen zusammenspielen, um bestehende Risiken zu identifizieren und daraus Informations- und IT-Sicherheitsmaßnahmen abzuleiten. Der Risikoprozess hat die Schutzbedürftigkeit der verarbeiteten personenbezogenen Daten zu berücksichtigen. Verfügbarkeit, Vertraulichkeit und Integrität sind zu wahren. Die Systeme müssen zudem belastbar ausgelegt werden.

Die abgeleiteten Maßnahmen können sowohl auf Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) beruhen als auch aus der ISO 27001 bzw. 27002 abgeleitet sein. Die Forderung, den derzeitigen Stand der Technik zu erfüllen, bedingt, dass zwingend ein PDCA-Zyklus zur ständigen Verbesserung der Maßnahmen etabliert wird. Im Rahmen der regelmäßigen Aktualisierung des VVT sind eine verfahrensbasierte Risikoanalyse und verfahrensspezifische Sicherheitsmaßnahmen erforderlich.

3.9 Sicherstellung privacy by design / by default

Neben den Anforderungen an die Transparenz der Datenverarbeitungsvorgänge, die durch entsprechende Pflichtinformationen gegenüber Betroffenen erreicht werden soll, ist die datenschutzfreundliche Ausgestaltung von Anwendungen und Systemen (‚privacy by design', ‚privacy by default) erklärtes Ziel der Datenschutzgesetzgebung.

‚Privacy by design' meint dabei Datenschutz durch Technikgestaltung und kann bei der konkreten Produkt- und/oder Anwendungsgestaltung nur durch frühzeitige, durchgängige und konsequente Berücksichtigung datenschutzrechtlicher Anforderungen erreicht werden. Typische Maßnahmen sind: Minimierung bzw. Pseudonymisierung personenbezogener Daten, Aufklärung der Nutzer über Funktionen und zugrundeliegende Datenverarbeitung, Implementierung von Löschroutinen, sichere Authentifizierungslösungen, etc.

‚Privacy by default' meint datenschutzfreundliche Grundeinstellungen. Nutzer der Anwendungen sollen jederzeit darauf vertrauen können, dass Datenschutz- und Datensicherheitsanforderungen schon durch die vorgegebene Konfiguration gewahrt sind.

3.10 Mitarbeitersensibilisierung

Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, soll auf den vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie verpflichtet werden. Mitarbeiter die besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis) unterliegen, werden ergänzend verpflichtet.

Durch flächendeckende Schulungen im Datenschutz soll ‚Basiswissen' in der Belegschaft aufgebaut werden. Personal, Marketing und andere Fachabteilungen können ergänzend speziell geschult werden. Unterweisungen werden in der Regel alle zwei Jahre angeboten, bei Neueinstellung oder Stellenwechsel erfolgt in der Regel eine Auffrischung.

4 Schlussbestimmungen

Die Einhaltung der Regelungen dieser Richtlinie gehört zu Ihren Arbeitspflichten. Verstöße können mit u.a. arbeitsrechtlichen Konsequenzen geahndet werden.

Für SPB Garant GmbH/SPB Deutschland GmbH

Fürth, im Januar 2026

Hr. Dominik Reising

Geschäftsführer

MUSTER: Anlage 2: Prozess Recht auf Berichtigung

Prozessbeschreibung:

1. Antrag der betroffenen Person

Die betroffene Person kann sich gem. Art. 16 DS-GVO mit ihrem Antrag auf Berichtigung an SPB Garant wenden. Hierbei kommen die unterschiedlichen Kommunikationskanäle (z. B. Post, E-Mail, Telefon) in Betracht. Es kann sein, dass hierbei die zentralen Kontaktdaten (Firmenimpressum) verwendet werden, es ist aber auch denkbar, dass sich ein bereits bestehender Geschäftskontakt an seinen Ansprechpartner in der jeweiligen Fachabteilung wendet. Anfragen können auch über info@spb-garant.de eingehen.

Den Antrag auf Berichtigung der Daten erkennen Sie daran, dass die Person die unverzügliche Berichtigung oder Vervollständigung ihrer Daten verlangt (z.B. weil sich ihre Adresse geändert hat).

2. Identitätsprüfung/Prüfprozess

Zunächst muss die Identität der betroffenen Person durch den Datenschutzkoordinator geklärt werden. Welche Methode geeignet ist, ist je nach Einzelfall zu beurteilen.

Kann die betroffene Person nicht identifiziert werden, ist diese vom Datenschutzkoordinator darüber zu unterrichten, damit sie ggf. zusätzliche Informationen bereitstellen kann, die eine Identifikation ermöglichen.

Aus Nachweiszwecken sollte die Unterrichtung per Post oder E-Mail erfolgen. Wichtig ist, dass auch die Gründe dokumentiert werden, warum die Person nicht identifiziert werden konnte.
Wenn trotz entsprechender Unterrichtung keine Identifikation möglich ist, besteht kein weiterer Handlungsbedarf mehr.

Wenn die Identitätsprüfung erfolgreich ist, so wird diese zum Nachweis dokumentiert und es ist mit Nr. 3 fortzufahren.

3. Weiterleitung an die zuständige Stelle

Der Antrag auf Berichtigung muss unverzüglich an info@spb-garant.de weitergeleitet werden. Dies geschieht per E-Mail.

Wichtig ist, dass der Antrag nachweislich und erkennbar weitergeleitet wird, daher muss eine E-Mail im Betreff besonders gekennzeichnet werden.
Für die Fristwahrung und Dokumentation ist es wichtig, in der E-Mail auch die Eingangszeit des Antrags sowie die Art des Eingangs zu vermerken. (z.B. Antrag telefonisch eingegangen am xx.xx.xxxx um xx Uhr).

Die zuständige Stelle prüft die Richtigkeit bzw. Vollständigkeit der Daten.

<table>
<tr><td colspan="3">Berichtigungsanspruch prüfen</td></tr>
<tr><td colspan="3">Vorprüfung: Warum werden welche Daten verarbeitet?
(Datenkategorien/ Verarbeitungszweck)</td></tr>
<tr><td>vollständig/ richtig</td><td>unrichtig</td><td>unvollständig</td></tr>
<tr><td rowspan="3">▼</td><td>▼</td><td>▼</td></tr>
<tr><td>Unverzügliche Korrektur</td><td>Ergänzung</td></tr>
<tr><td>▼</td><td>▼</td></tr>
<tr><td>Info, dass kein Anspruch besteht</td><td>Info, dass korrigiert wurde</td><td>Info, dass ergänzt wurde</td></tr>
</table>

4. Einbindung des Datenschutzbeauftragten

Bei Unklarheiten ist der Datenschutzbeauftragte einzubinden.

5. Umsetzung / Antwort an die betroffene Person

Wenn die Daten unrichtig bzw. unvollständig gespeichert waren, werden diese durch den Datenschutzkoordinator entsprechend korrigiert bzw. vervollständigt.

Die betroffene Person ist durch den Datenschutzkoordinator unverzüglich bzw. spätestens innerhalb eines Monats nach Eingang des Antrags zu informieren, ob die Daten berichtigt bzw. vervollständigt wurden.
Wenn der Antrag nicht umgesetzt wurde, sind der betroffenen Person die Gründe mitzuteilen. Ferner muss sie auf die Möglichkeit hingewiesen werden, bei einer Datenschutzaufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

Ausnahmsweise kann die Rückmeldung innerhalb von zwei weiteren Monaten erfolgen, wenn die Anzahl der Anträge und deren Komplexität es erforderlich macht. In diesem Fall muss die betroffene Person aber durch den Datenschutzkoordinator innerhalb eines Monats nach

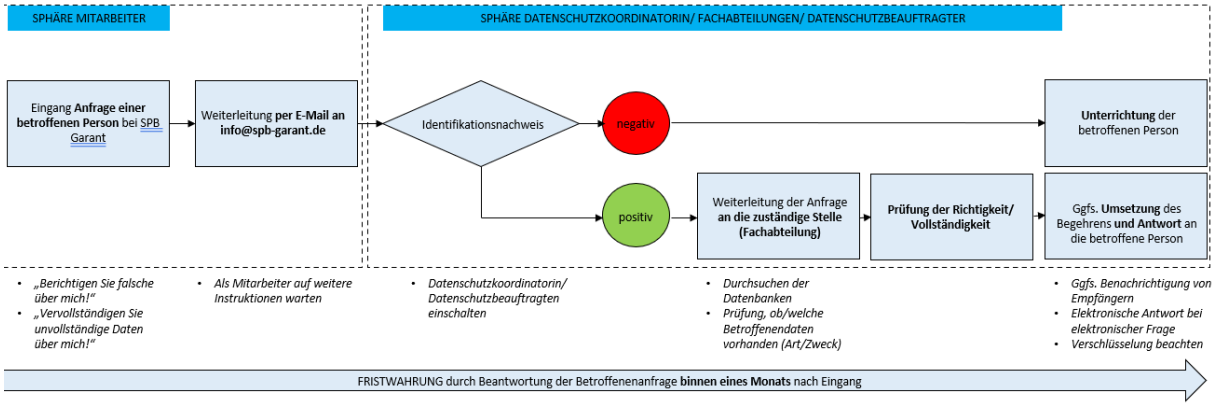
seinem Antrag darüber informiert werden, dass die Bearbeitung länger dauern wird; die Gründe für die Verzögerung sind ebenfalls zu nennen.

Sofern auch anderen Unternehmen diese unrichtigen Daten übermittelt worden sind, müssen diese ebenfalls nachweislich durch den Datenschutzkoordinator informiert werden, dass die Daten berichtigt bzw. vervollständigt wurden.
Hiervon kann nur abgesehen werden, wenn der Vorgang unmöglich ist oder einen unverhältnismäßigen Aufwand bedeutet. Dies muss aber ebenfalls plausibel begründet und zum Nachweis dokumentiert werden.

Stellt die betroffene Person den Antrag auf Berichtigung elektronisch (z. B. E-Mail), so ist auch die Rückmeldung in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern nichts Abweichendes von der betroffenen Person gewünscht ist.

Auch hier gilt, dass der Antrag auf Berichtigung bzw. Umsetzung unentgeltlich erfolgt. Nur bei offenkundig unbegründeten oder exzessiven Anträgen (im Falle häufiger Wiederholung) kann ein Entgelt verlangt werden. Alternativ kann in diesen Fällen auch der Antrag verweigert werden. SPB Garant hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen. In diesen Sonderfällen ist jedoch stets mit dem Datenschutzbeauftragten Rücksprache zu halten. Denn wenn der Antrag doch begründet war und nicht fristgerecht erteilt wurde, kann ein Bußgeld verhängt werden.

Schaubild:



zurück