Datenschutzrichtlinie der BMS Building Materials Suisse

in Übereinstimmung mit der EU-Datenschutz-Grundverordnung und dem Schweizerischen Datenschutzgesetz

Abteilung:	Legal & Compliance
Verfasser:	Christina Hooker, Legal Counsel
Erstellt:	September 2022

Diese Datenschutzrichtlinie enthält Vorschriften zum Schutz personenbezogener Daten, die für alle Unternehmen unter der Dachmarke BMS Building Materials Suisse (**BMS Unternehmen**) gelten. Sie legt die Bedeutung und den Stellenwert des Datenschutzes im Sinne der Achtung der Grundrechte und Grundfreiheiten der Mitarbeitenden, Kunden und Geschäftspartner der BMS Unternehmen fest.

Als Grundlage für diese Datenschutzrichtlinie dienen die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, die Datenschutz-Grundverordnung (**DSGVO**) sowie das schweizerische Bundesgesetz inkl. Verordnungen über den Datenschutz (**DSG**).

Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten innerhalb des Europäischen Binnenmarktes sowie zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 DSGVO). Sie gilt unmittelbar in allen EU-Mitgliedstaaten seit dem 25. Mai 2018.

Nach Art. 3 Abs 1 DSGVO findet diese Verordnung Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet. Da die BMS Unternehmen als Gruppengesellschaft der BME Gruppe unterstehen, welche ihren Sitz in der Union hat, und da BME beschlossen hat, dass die DSGVO gruppenweit umzusetzen ist, ist die DSGVO für die BMS Unternehmen relevant und die BMS Unternehmen haben bei der Verarbeitung von personenbezogenen Daten deren Vorgaben einzuhalten.

Als Unternehmen mit Schweizer Niederlassungen unterstehen die BMS Unternehmen selbstverständlich auch dem schweizerischen Datenschutzgesetz.

Was du wissen musst

Die Datenschutz-Grundverordnung und das Schweizerische Datenschutzgesetz regeln, wie persönliche Daten geschützt werden sollen, wenn sie von jemand anderem (Person oder Unternehmen) als der Person selbst verarbeitet werden.

Da die Gruppe, welcher wir unterstehen, die BME Building Materials Europe, ihren Sitz in den Niederlanden hat – ein Land der Europäischen Union - und Datenschutz homogen gruppenweit umsetzen möchte unterstehen auch wir der DSGVO. Ausserdem unterstehen wir als Schweizer Unternehmen dem schweizerischen DSG.

Inhalt

1. Gegenstand

Gegenstand dieser Datenschutzrichtlinie ist die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, unabhängig von der Art ihrer Verarbeitung und der Form (Papier, digital, mündlich), sofern die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen (vgl. Art. 2 Abs. 1 DSGVO, Art. 1 DSG).

2. Geltungsbereich

Diese Datenschutzrichtlinie gilt für alle Mitarbeitenden der BMS Unternehmen, die personenbezogene Daten verarbeiten.

Die Mitarbeitenden werden im Rahmen ihres Arbeitsvertrages verpflichtet, die relevanten datenschutzrechtlichen Bestimmungen sowie diese Datenschutzrichtlinie einzuhalten. Externe Personen und Gesellschaften sowie Geschäftspartner, die im Auftrag eines BMS Unternehmens personenbezogene Datengruppen verarbeiten, werden vertraglich zur Einhaltung der sie betreffenden Datenschutzbestimmungen verpflichtet.

Diese Datenschutzrichtlinie dient ebenfalls für die Verarbeitung von personenbezogenen Daten von Mitarbeitenden der BMS Unternehmen. Alle Mitarbeitenden erhalten mit dem Arbeitsvertrag ein Datenschutzhinweis, der sie darüber informiert, welche ihrer Personendaten von den BMS Unternehmen zu welchem Zweck bearbeitet werden und welche Rechte sie diesbezüglich haben.

Was du wissen musst

Personenbezogene Daten sind: Informationen, die eine lebende Person betreffen und es ermöglichen, diese Person zu identifizieren, wie z. B. Vorname und Nachname, Adresse, Geburtsdatum, Telefonnummer, Kontonummer, Berufsbezeichnung, Foto, unter Umständen auch IP-Adressen, u.a.

Verarbeitung bedeutet: Jeder Vorgang an solchen personenbezogenen Daten wie das Erheben, Erfassen, die Organisation, das Ordnen, das Speichern, das Anpassen oder Abändern, das Auslesen, das Abfragen, das Verwenden, das Übermitteln/Teilen/Verbreiten oder sonst wie Bereitstellen, das Vergleichen oder Verknüpfen, das Einschränken, Löschen oder Vernichten.

Diese Richtlinie dient zu Deinem Schutz als Mitarbeitender der BMS, sie dient aber auch dazu, Dich zum Schutz der Personendaten anderer zu verpflichten; sie beinhaltet Regeln, welche Du befolgen musst, wenn Du Daten unserer Kunden, Geschäftspartner, Lieferanten, Dienstleister aber auch Webseitenbesucher verarbeitest.

3. Verzeichnis von Verarbeitungstätigkeiten

Die BMS Unternehmen führen ein Verzeichnis der Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses enthält mindestens folgende Angaben:

a. den Namen und die Kontaktdaten des jeweiligen BMS Unternehmen, bzw. des jeweilig zuständigen Departementes
b. die Zwecke der Verarbeitung
c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
d. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschliesslich Empfänger in Drittländern
e. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland, einschliesslich der Angabe des betreffenden Drittlands
f. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
g. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen gemäss Art. 32 Abs. 1 DSGVO, Art. 11 DSG.

Was du wissen musst

Wir führen ein Verzeichnis in dem wir alle Vorgänge, mit denen personenbezogene Daten (unserer Mitarbeitenden, unserer Kunden, unserer Geschäftspartner, etc.) verarbeitet werden, auflisten. Dieses Verzeichnis ist wichtig, denn es gibt uns ein Überblick darüber, wie wir welche Personen-daten in welchen Verarbeitungsvorgängen schützen, wer im Unternehmen für den Schutz zuständig ist und was genau an personenbezogenen Daten verarbeitet werden. Auch wird diese Liste im Falle einer Due Diligence durch eine Aufsichtsbehörde vorgewiesen.

4. Grundsätze für die Verarbeitung von personenbezogenen Daten

Die BMS Unternehmen halten bei der Verarbeitung von personenbezogenen Daten die folgenden Grundsätze ein:

- **Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  Personenbezogene Daten müssen auf rechtmässige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Art. 5 Abs. 1 litera a DSGVO, Art. 4 Absätze 1,2,3 DSG).

- **Zweckbindung**
  Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (vgl. Art. 5 Abs. 1 lit b DSGVO, Art. 4 Abs. 3 DSG).

- **Datenminimierung**
  Personenbezogene Daten müssen dem Zweck angemessen und erheblich sein sowie auf das für die Zwecke der Verarbeitung notwendige Mass beschränkt sein (vgl. Art. 5 Abs.1 lit c DSGVO, Art. 4 Abs. 3 DSG).

- **Richtigkeit**
  Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein (vgl. Art. 5 Abs. 1 lit d DSGVO, Art. 4 Abs. 5 DSG).

- **Speicherbegrenzung**
  Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (vgl. Art. 5 Abs.1 lit e DSGVO, Art. 4 Abs. 4 DSG).

- **Integrität und Vertraulichkeit**
  Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschliesslich Schutz durch geeignete technische und organisatorische Massnahmen vor unbefugter oder unrechtmässiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung (vgl. Art. 5 Abs. 1 lit f DSGVO).

- **Rechenschaftspflicht**
  Die BMS Unternehmen sorgen dafür, dass die oben genannten Grundsätze für alle personenbezogenen Daten eingehalten werden und können dies nachweisen (vgl. Art. 5 Abs. 2 DSGVO)

4.1 Rechtmässigkeit der Verarbeitung

Die BMS Unternehmen verarbeiten personenbezogene Daten nur, wenn mindestens eine der Bedingungen gemäss Art. 6 Abs. 1 DSGVO und Art. 24 DSG erfüllt ist, insbesondere:

- Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

- die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Massnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

- die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der das jeweilige BMS Unternehmen unterliegt;
- die Verarbeitung ist zur **Wahrung der berechtigten Interessen des jeweiligen BMS Unternehmen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Überwiegende Interessen des jeweiligen BMS Unternehmens sind gemäss Art. 24 Abs 2 DSG insbesondere dann gegeben,
    - wenn dieses mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben;
    - wenn Personendaten zur Prüfung der Kreditwürdigung der betroffenen Person (Kunden) bearbeitet werden (und es sich dabei nicht um besonders schützenswerte Personendaten handelt, nur die für den Abschluss oder die Abwicklung eines Vertrags mit der betroffenen Person notwendigen Daten bekanntgegeben werden und die betroffene Person volljährig ist)

4.2 Bedingungen für die Einwilligung

- Das jeweilige BMS Unternehmen holt die notwendigen Einwilligungen der betroffenen Personen rechtzeitig ein.
- Die Einwilligung erfolgt durch eine eindeutige bestätigende Handlung, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
- Eine Einwilligungserklärung wird in verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache zur Verfügung gestellt. Sie ist von anderen Angelegenheiten klar unterscheidbar und beinhaltet keine missbräuchlichen Klauseln.
- Ausserdem wird der betroffenen Person eine einfache Methode zur Verfügung gestellt, mit der sie ihre Einwilligung jederzeit widerrufen kann.

4.3 Anforderungen an die Zweckbestimmung

- Die personenbezogenen Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
- Unter gewissen Umständen können personenbezogene Daten zu weiteren Zwecken verarbeitet werden, die über den ursprünglichen Verarbeitungszweck zum Zeitpunkt der Datenerhebung hinausgehen, diese müssen im Verzeichnis aufgenommen und falls nötig den betroffenen Personen kommuniziert werden.

4.4 Verarbeitung personenbezogener Daten eines Kindes

- Die BMS Unternehmen verarbeiten grundsätzlich nur personenbezogene Daten eines Kindes, welches das sechszehnte Lebensjahr vollendet hat.
- Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, verarbeiten die BMS Unternehmen dessen personenbezogenen Daten nur, sofern und soweit die Einwilligung zur Verarbeitung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.

4.5 Verarbeitung besonderer Kategorien personenbezogener Daten

- Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person oder Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, ist ohne ausdrückliche Einwilligung grundsätzlich untersagt (Art. 9 Abs. 1 DSGVO, Art. 4 Abs 6 DSG).
- Die BMS Unternehmen verarbeiten, wenn überhaupt, besondere Kategorien von personenbezogenen Daten ausschliesslich von Mitarbeitenden und ausschliesslich im Zusammenhang mit der Organisation der Geschäftstätigkeit und zur Einhaltung und Überprüfung von arbeits- und sozialversicherungsrechtlichen Verpflichtungen. Für die Verarbeitung dieser Kategorie personenbezogener Daten wird die ausdrückliche Einwilligung der betroffenen Person eingeholt, wenn kein anderer Rechtfertigungsgrund vorliegt.

4.6 Digital Marketing

- Die BMS Unternehmen senden keine Mitteilungen zu Werbe- oder Marketingzwecken an Kontakte über digitale Medien wie Mobiltelefonie, E-Mail oder Internet, ohne die Zustimmung der betroffenen Personen einzuholen.
- Wenn eine Einwilligung zur Verarbeitung von personenbezogenen Daten zu digitalen Marketingzwecken vorliegt, wird die betroffene Person bei der ersten Datenerhebung darüber informiert, dass sie das Recht hat, jederzeit die Verarbeitung ihrer personenbezogenen Daten zu solche Zwecken zu widerrufen.

4.7 Speicherungsdauer

- Die BMS Unternehmen speichern personenbezogene Daten nicht länger, als es für die Zwecke, zu denen sie ursprünglich erhoben oder später weiterverarbeitet wurden, notwendig ist (vgl. Art. 5 Abs. 1 lit. e DSGVO, Art. 4, Abs. 4 DSG).
- Was als notwendig gilt, hängt von den Umständen im Einzelfall ab, unter Berücksichtigung der Gründe, aus denen die personenbezogenen Daten erhoben wurden.

Was du wissen musst

Wir halten uns an die Grundsätze der DSGVO und der DSG: Wir wollen Personendaten **rechtmässig** verarbeiten, nur zu **klar festgelegten Zwecken** (und nicht darüber), nur **so viele** Personendaten **wie absolut notwendig**, nur **richtige** Personendaten, wir wollen Personendaten nur **solange wie notwendig speichern** und wir wollen sie möglichst gut vor Verlust, Zerstörung, Schädigung und unrechtmässiger Verbreitung **schützen**.

Personendaten sind rechtmässig verarbeitet wenn die Verarbeitung einem **gültigen Rechtsgrund** unterliegt (DSGVO) oder einen **Rechtfertigungsgrund** hat (DSG), dies ist insbesondere dann der Fall, wenn die Personendaten verarbeitet werden um einen **Vertrag** oder eine **rechtliche Pflicht zu erfüllen**, um unsere **berechtigten Wirtschaftsinteressen zu erfüllen** (vorausgesehen diese wiegen schwerer als die Grundrechte-und freiheiten der betroffenen Person) oder wenn wir eine **Einwilligung** von der betroffenen Person erhalten haben, nachdem sie klar über die Verarbeitung ihrer Personendaten informiert wurde. Eine Einwilligung muss vor allem bei Verarbeitungen im Rahmen von Marketingmassnahmen eingeholt werden.

Für eine **gültige Einwilligung** musst Du:

- sie rechtzeitig einholen
- dafür sorgen, dass die Einwilligung eindeutig ist und für einen konkreten Fall gegeben wird. Z. B. muss eine Einwilligungsmöglichkeit gleich unter der Eingabe von Personendaten für das Bestellen eines Newsletters stehen, mittels einer Checkbox, welche proaktiv angekreuzt werden muss, nicht bereits angekreuzt ist
- dafür sorgen, dass die Einwilligungserklärung klar und leicht verständlich ist, damit die betroffene Person wirklich korrekt informiert ist bevor sie einwilligt
- die Möglichkeit geben, die Einwilligung jederzeit zurückzuziehen. Z. B. muss man sich am Ende eines jeden Newsletters mit 1 – 2 Mausklick wieder abmelden können.

Bei Lehrlingen, die noch nicht 17 sind, ist von den Eltern eine informierte Einwilligung zur Verarbeitung der Personendaten ihres Kindes zu verlangen.

Besonders sensible Personendaten werden bei uns nur von der HR Abteilung verarbeitet. Diese Daten werden dementsprechend auch besonders gut geschützt und die HR Mitarbeitenden sind dahingehend geschult.

5. Rechte der betroffenen Personen

Einzelpersonen, deren Personendaten verarbeitet werden, stehen nach der DSGVO und der DSG bestimmte Rechte zu.

5.1 Informationspflicht

Das jeweilige BMS Unternehmen teilt der betroffenen Person zum Zeitpunkt der Erhebung der personenbezogenen Daten Folgendes mit (vgl. Art. 13 Abs 1 DSGVO, Art. 19 DSG): Ihren **Namen und Kontaktdaten**, die **Zwecke**, für welche die personenbezogenen Daten verarbeitet werden sollen sowie die **Rechtsgrundlage** für die Verarbeitung oder gegebenenfalls die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden (nur nach DSGVO), gegebenenfalls die **Empfänger** der personenbezogenen Daten und gegebenenfalls die Absicht, die personenbezogenen Daten an ein **Drittland** zu übermitteln. Nach Schweizer DSG muss das jeweilige Unternehmen zudem, wenn Personendaten ins Ausland bekanntgegeben werden, den betroffenen Personen auch den **Staat und gegebenenfalls die Garantien** (zum Schutz der Personendaten im Ausland) mitteilen.

Zusätzlich stellt das jeweilige BMS Unternehmen der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten: Die **Speicherdauer** oder falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer, das Bestehen eines **Rechts auf Auskunft**, auf **Berichtigung** und **Löschung**, auf **Einschränkung der Verarbeitung** und auf **Widerspruch** und wenn eine Einwilligung eingeholt wurde das Recht, die **Einwilligung jederzeit zu widerrufen** (ohne dass die Rechtmässigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird) sowie das Bestehen eines **Beschwerderechts** bei der Aufsichtsbehörde.

5.2 Auskunftsrechte

Alle betroffenen Personen, von denen die BMS Unternehmen personenbezogene Daten verarbeiten, haben – nach Stellen einer schriftlichen Anfrage via E-Mail an **dataprotection@bmsuisse.ch** und Überprüfung ihrer Identität – das Recht, vom jeweiligen BMS Unternehmen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat die betroffene Person das Recht, alle in Art. 15 Abs.1 DSGVO, Art. 25 DSG genannten Informationen bezüglich ihrer eigenen personenbezogenen Daten zu erhalten. Dies sind:

- Identität und Kontaktdaten unseres Unternehmens
- Verarbeitungszweck
- Kategorien personenbezogener Daten
- Empfänger, gegenüber denen die personenbezogenen Daten offengelegt worden sind, insbesondere bei Empfängern in Drittländern
- Angaben zu Exporten wie eine Länderliste und Rechtsgrundlagen (nur gemäss Schweizer DSG)
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder ansonsten die Kriterien für die Festlegung dieser Dauer

- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch das jeweilige BMS Unternehmen oder eines Widerspruchrechts gegen diese Verarbeitung
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden dann alle verfügbaren Informationen über die Herkunft der Daten.
- falls personenbezogene Daten an ein Drittland übermittelt werden und diesbezüglich geeignete Garantien für die Übermittlung vorgesehen werden müssen, so hat die betroffene Person das Recht, über diese Garantien unterrichtet zu werden.

Durch die Weitergabe der angefragten Informationen an die betroffene Person könnten unter gewissen Umständen personenbezogene Daten einer anderen betroffenen Person offengelegt werden.
In solchen Fällen müssen die betreffenden Informationen redigiert oder zurückbehalten werden, je nachdem was notwendig oder angemessen erscheint, um die Rechte dieser Person zu schützen.

Die BMS Unternehmen können nach Schweizer DSG die Auskunft verweigern, einschränken oder aufschieben, wenn:

- ein Gesetz im formellen Sinn dies vorsieht, namentlich um ein Berufsgeheimnis zu schützen;
- dies aufgrund überwiegender Interessen Dritter erforderlich ist; oder
- das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist.

Auskunftsgesuche von betroffenen Personen werden gemäss **Prozessablauf**

verarbeitet und mittels des entsprechenden **Formulars** an dataprotection@bmsuisse.ch gestellt.

5.3 Profiling/Automatisierte Entscheidungen im Einzelfall

Die BMS Unternehmen wenden Profiling nur im aktuellen HRIS-Tool der BMS an. Das Profiling erfolgt mit der ausdrücklichen Einwilligung der betroffenen Personen oder für die Erfüllung der Verträge zwischen den betroffenen Personen und den BMS Unternehmen und es werden angemessene Massnahmen getroffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Perso-nen zu schützen.

5.4 Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem jeweiligen BMS Unternehmen die Berichtigung sie betreffender personenbezogener Daten zu verlangen. Darunter fällt auch das Recht, die Vervollständigung/Ergänzung unvollständiger personenbezogener Daten zu verlangen (unter Berücksichtigung der Verarbeitungszwecke). Anfragen werden gemäss **Prozessablauf** verarbeitet und mittels des entsprechenden **Formulars** an dataprotection@bmsuisse.ch gestellt.

5.5 Recht auf Löschung

Betroffene Personen haben unter gewissen Voraussetzungen das Recht, vom jeweiligen BMS Unternehmen zu verlangen, dass sie betreffende personenbezogene Daten gelöscht werden (eine unwiderrufliche Anonymisierung ist einer Löschung gleichzusetzen), und
das jeweilige Unternehmen ist verpflichtet, personenbezogene Daten zu löschen/unwiderruflich zu anonymisieren, sofern eines der folgenden Gründe zutrifft (vgl. Art. 17 Abs 1 DSGVO, Art. 32 Abs. 2 lit c DSG):

- Die personenbezogenen Daten sind für den Erhebungszweck nicht mehr notwendig
- Die betroffene Person widerruft ihre Einwilligung und es fehlt an einer anderen Rechtsgrundlage für die Verarbeitung
- Die betroffene Person legt Widerspruch ein gegen die Verarbeitung und es liegen keine berechtigenden Gründe für die Verarbeitung vor
- Die personenbezogenen Daten wurden unrechtmässig verarbeitet
- Die Löschung der personenbezogenen Daten ist nach Schweizer Recht erforderlich

Das Recht zur Löschung personenbezogener Daten besteht nicht, soweit die Verarbeitung erforderlich ist:

- zur Ausübung des Rechts auf freie Meinungsäusserung und Information
- zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem jeweiligen BMS Unternehmen übertragen wurde
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Anfragen auf Löschung werden gemäss **Prozessablauf** verarbeitet und mittels des entsprechenden **Formulars** an dataprotection@bmsuisse.ch gestellt.

Was du wissen musst

Jede betroffene Person deren Personendaten verarbeitet werden, hat folgende **Rechte**:

- Das Recht korrekt und vollständig informiert zu werden, insbesondere: Über die Verarbeitung und den Verarbeiter, über alle bestehenden Rechte, über eine Erweiterung des Verarbeitungszwecks und über die jederzeitige Widerrufsmöglichkeit einer jeden Einwilligung
- Das Recht als betroffene Person Auskunft zu erhalten darüber, ob und welche Personendaten wie verarbeitet werden
- Das Recht, falsche oder unvollständige Personendaten berichtigen oder ergänzen zu lassen
- Das Recht Personendaten löschen zu lassen, wenn
    - sie nicht mehr notwendig sind
    - keine Einwilligung mehr besteht
    - gegen die Verarbeitung Widerspruch eingelegt wurde
    - die Verarbeitung unrechtmässig war
    - ein Schweizer Gesetz das Löschen vorsieht

Links zu den Prozessen und Formularen finden sich im vorangehenden Kapitel.

Ausgefüllte Auskunftsbegehren, Berichtigungs-/Änderungsbegehren und Löschbegehren sind per E-Mail an dataprotection@bmsuisse.ch zu stellen.

6. Übermittlung personenbezogener Daten an Dritte

6.1 Grundsatz

Eine Übermittlung personenbezogener Daten an ein Drittland darf vorgenommen werden, wenn das betreffende Drittland ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung (vgl. Art. 45 DSGVO, Art. 16 f DSG).

Falls kein Angemessenheitsbeschluss der Kommission vorliegt, dürfen die BMS Unternehmen personenbezogene Daten an ein Drittland nur übermitteln, sofern diese geeignete Garantien vorgesehen haben und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe

zur Verfügung gestellt werden (vgl. Art. 46 DSGVO, Art. 16 Abs. 2 DSG).

Falls weder ein Angemessenheitsentscheid und noch geeignete Garantien vorliegen, so übermitteln die BMS Unternehmen personenbezogene Daten nur an ein Drittland wenn gewisse Voraussetzungen erfüllt sind, hierunter die wichtigsten:

- die betroffene Person hat in die Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die bestehenden möglichen Risiken ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde
- die Übermittlung ist für die Erfüllung eines Vertrages zwischen der betroffenen Person und dem jeweiligen BMS Unternehmen oder zur Durchführung von vorvertraglichen Massnahmen auf Antrag der betroffenen Person erforderlich

6.2 Übermittlungen zwischen BMS und BME oder anderen Unternehmen unter BME

Für die effiziente Ausführung der Geschäftstätigkeiten der BMS Unternehmen kann es notwendig sein, dass personenbezogene Daten an BME oder an andere Unternehmen unter BME übermittelt werden oder BME Zugang zu personenbezogenen Daten gewährt wird. Insbesondere können Personaldossiers von BMS-Mitarbeitenden zum Zweck der Vergütung von Führungskräften und der Entwicklung/ Schulung von Mitarbeitenden in die Personalabteilung der BME nach Amsterdam übermittelt werden. Dabei werden die zum Schutz der personenbezogenen Daten notwendigen Massnahmen bei jeder Übermittlung getroffen.

Wenn sich das Unternehmen, welches die Daten empfängt, in einem Drittland befindet, dann wendet das jeweilige BMS Unternehmen Übermittlungsmechanismen an, die den betroffenen Personen rechtsverbindliche und durchsetzbare Rechte bezüglich der Verarbeitung ihrer personenbezogenen Daten gewähren (Standarddatenschutzklauseln) oder holt sich die ausdrückliche Einwilligung der umfänglich informierten betroffenen Personen zur Übermittlung ein.

Insbesondere sorgen die BMS Unternehmen und ihre Mitarbeitenden dafür, dass

- vor der Übermittlung in ein Drittland die Genehmigung von Legal & Compliance eingeholt wird
- nur die Mindestmenge an personenbezogenen Daten, die für den Zweck der Übermittlung notwendig ist, übermittelt wird
- angemessene Sicherheitsmassnahmen getroffen werden, um die personenbezogenen Daten während der Übermittlung zu schützen

6.3 Übermittlungen an sonstige Dritte

Die BMS Unternehmen übermitteln personenbezogene Daten an Dritte und gewähren Dritten Zugang zu personenbezogenen Daten nur, wenn garantiert ist, dass die Daten vom Empfänger rechtmässig verarbeitet und angemessen geschützt werden.

Falls eine Verarbeitung von personenbezogenen Daten durch einen Dritten stattfindet, klärt die betreffende BMS Unternehmung zuerst ab, ob gemäss geltendem Recht der Dritte als Verantwortlicher oder Auftragsverarbeiter der betreffenden personenbezogenen Daten gilt.

Gilt der Dritte als Verantwortlicher, so schliesst das jeweilige BMS Unternehmen einen Vertrag für gemeinsam Verantwortliche ab, welcher die Verantwortlichkeiten bezüglich der übermittelten personenbezogenen Daten jeder Partei definiert.

Gilt der Dritte als Auftragsverarbeiter, so schliesst das jeweilige BMS Unternehmen einen Datenverarbeitungsvertrag ab und verpflichtet darin den Dritten die datenschutzrechtlichen Grundsätze einzuhalten. (vgl. Art. 28 DSGVO, Art. 9 DSG)

Unter gewissen Umständen ist es erlaubt, personenbezogene Daten ohne das Wissen oder die Einwilligung der betroffenen Person weiterzugeben, unter anderem wenn dies notwendig ist für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung.

Was du wissen musst

Es können Personendaten auch in ein anderes Land verschickt und dort verarbeitet werden. Dieses Land muss jedoch Gesetze haben, welche einen angemessenen Schutz dieser versendeten Personendaten garantieren. Alle Länder der europäischen Union erfüllen diese Voraussetzung, denn sie unterliegen der DSGVO. Auch die Schweiz und das Vereinigte Königreich zum Beispiel haben Gesetze, die angemessenen Schutz garantieren. Hier dürfen Daten ohne besondere Genehmigung übertragen werden.

Dies gilt auch für eine Übermittlung von Personendaten an unsere Muttergesellschaft BME. Selbstverständlich werden auch bei einer Übermittlung in ein sogenanntes datensicheres Land Datenverarbeitungsverträge oder Datentransferverträge unterschrieben, die garantieren, dass die Personendaten bei der Übermittlung und Verarbeitung angemessen geschützt werden, jedoch sind keine weiteren Massnahmen notwendig.

Die USA und gewisse andere Länder hingegen, können keinen angemessenen Schutz von Personendaten garantieren. Hier braucht es eine separate Genehmigung. Meistens geschieht dies durch eine ausdrückliche Einwilligung der betroffenen Person (die vorher klar darüber informiert wurde, dass ihre Personendaten in ein datenunsicheres Land transferiert und/oder verarbeitet werden), oder – wenn es um Personendaten mehrerer Personen geht – durch die Vereinbarung von sogenannten Standarddatenschutzklauseln, die zusätzliche Schutzmassnahmen garantieren.

Wenn wir Personendaten mit Dienstleistern (Logistik, IT, etc.), Lieferanten, Geschäftspartnern und sonstigen Dritten teilen, so garantieren wir mittels Auftragsdatenverarbeiterverträgen, dass diese Personendaten angemessen geschützt werden.

7. Technische und organisatorische Massnahmen

Die BMS Unternehmen treffen angemessene technische und organisatorische Massnahmen um die Sicherheit der personenbezogenen Daten gemäss den anwendbaren datenschutzrechtlichen Vorschriften zu gewährleisten. Die jeweilig getroffenen Massnahmen werden im Verzeichnis hinter der betreffenden Verarbeitung festgehalten.

8. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (privacy by design und privacy by default)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, treffen die BMS Unternehmen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Massnahmen (wie z. B. Pseudonymisierung), die dafür ausgelegt sind, die Datenschutzgrundsätze gemäss Kapitel 4 dieser Datenschutzrichtlinie wirksam umzusetzen und die notwendigen Garantien zum Schutz der Rechte der betroffenen Personen in die Verarbeitung aufzunehmen (Art. 25 Abs. 1 DSGVO, Art. 7 DSG).

Die BMS Unternehmen treffen geeignete technische und organisatorische Massnahmen, damit durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Massnahmen betreffen die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit und stellen insbesondere sicher, dass personenbezogene Daten durch Voreinstellungen nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden (Art. 25 Abs. 2 DSGVO, Art. 7 Abs. 3 DSG).

Um sicherzustellen, dass alle Datenschutzgrundsätze bei der Entwicklung, Abänderung oder Erweiterung von Systemen oder Prozessen berücksichtigt werden, müssen diese Systeme oder Prozesse vor (Weiter)-Gebrauch einen Genehmigungsprozess durchlaufen. Für alle neuen oder abgeänderten Systeme oder Prozesse wird auch eine Datenschutz-Folgenabschätzung im Sinne von Kapitel 10 dieser Datenschutzrichtlinie durchgeführt.

9. Sensibilisierung und Schulung der Mitarbeitenden

Die BMS Unternehmen führen angemessene interne Prozesse und Mechanismen zur Einbindung und Bewusstseinsbildung der Mitarbeitenden ein.

Alle Mitarbeitenden der BMS Unternehmen, die Zugang zu personenbezogenen Daten haben, sind entsprechend gemäss dieser Datenschutzrichtline in die Verantwortung genommen. Sie werden im Rahmen der Mitarbeitereinführung auf die Datenschutzrichtlinie hingewiesen und stimmen dem Datenschutzhinweis zu. Die BMS Unternehmen unterstützen ihre Mitarbeitenden bei den betreffenden Prozessen und führen zudem Datenschutzschulungen durch, die mindestens den folgenden Inhalt haben:

a) Die Grundsätze der Verarbeitung personenbezogener Daten gemäss Kapitel 4 dieser Datenschutzrichtlinie;

b) Die Verantwortung jedes Mitarbeitenden, dafür zu sorgen, dass personenbezogene Daten nur von autorisierten Personen und zu bewilligten Zwecken verarbeitet werden;

c) Die Notwendigkeit und korrekte Anwendung der Formulare und Prozesse, die zur Umsetzung dieser Datenschutzrichtlinie genehmigt wurden;

d) Die korrekte Anwendung von Passwörtern, Security Tokens und anderen Zugangsmechanismen;

e) Die Wichtigkeit, den Zugang zu personenbezogenen Daten zu limitieren, z. B. durch passwortgeschützte Bildschirmschoner und Ausloggen;

f) Sichere Lagerung von physischen Akten und elektronischen Speichermedien;

g) Die Notwendigkeit einer entsprechenden Genehmigung und angemessener Sicherheitsmassnahmen für alle Übermittlungen von personenbezogenen Daten ausserhalb des internen Netzwerkes und der Geschäftsräumlichkeiten;

h) Richtige Entsorgung der personenbezogenen Daten

i) Spezifische Risiken in Bezug auf personenbezogene Daten im Zusammenhang mit den betreffenden Aktivitäten oder Aufgaben einer Abteilung.

Bestehen Unklarheiten bezüglich Verarbeitung oder Weitergabe von personenbezogenen Daten, kann der Mitarbeitende sich über dataprotection@bmsuisse.ch an Legal & Compliance wenden.

Was du wissen musst

Wir schützen Personendaten unserer Mitarbeiter, unserer Kunden und unserer Geschäftspartner mittels technischer und organisatorischer Massnahmen.

Für die **technischen Massnahmen** ist vor allem unsere IT Abteilung zuständig; sie sorgen dafür, dass wir auf einem hohen Stand der Technik bleiben, dass wir vor externen und internen Angriffen geschützt sind, dass nur die wirklich notwendigen Personendaten gesehen/geteilt werden können und dass die nicht mehr benötigten Personendaten gelöscht werden.

Damit unser Schutzniveau hoch bleibt werden neue Verarbeitungen mittels einer Datenschutz-Folgenabschätzung überprüft und dabei die notwendigen Schutzmassnahmen eruiert.

Für die **organisatorischen Massnahmen** sind alle Mitarbeitenden verantwortlich und es ist auch unsere ICT Weisung zu beachten: Es handelt sich um Massnahmen wie das Sperren des Computerbildschirms, das Abschliessen von Dokumentenablagen, die Wahl eines starken Passwortes, aber auch die Sensibilisierung und Schulung der Mitarbeitenden, welche Personendaten verarbeiten.

Für mehr Information zu den technischen und organisatorischen Massnahmen oder zu den angebotenen Schulungen kannst du dich per E-Mail an dataprotection@bmsuisse.ch wenden.

10. Datenschutz-Folgenabschätzung

Das jeweilige BMS Unternehmen führt vorab eine Abschätzung der Folgen von vorgesehenen Verarbeitungsvorgängen durch, wenn die Form der betreffenden Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat (Art.35 Abs. 1 DSGVO, Art. 22 DSG).

Die Datenschutz-Folgenabschätzung hat mindestens folgenden Inhalt (vgl. Art.35 Abs. 7 DSGVO, Art. 22 Abs. 3 DSG):

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung;

b) eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

d) die zur Bewältigung der Risiken geplanten Abhilfemassnahmen, einschliesslich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten und der Nachweis der DSGVO und DSG-Konformität sichergestellt wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Der jeweilige Mitarbeitende, der für die Einführung einer neuen Verarbeitung (bspw. neue App, neue Plattform, neue Kameras, neuer E-Shop, etc) zuständig ist, holt bei der Entscheidfindung, ob eine Durchführung einer Datenschutz-Folgenabschätzung notwendig ist, den Rat von Legal & Compliance ein. Es sind die Schritte gemäss **Konzept zur Datenschutz-Folgenabschätzung** zu befolgen.

11. Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten von Personen, die sich in der Europäischen Union befinden, meldet der jeweilige Mitarbeitende, der die Verletzung entdeckt/dem die Verletzung gemeldet wurde, diese Verletzung unverzüglich nach Kenntnisnahme zuerst intern an dataprotection@bmsuisse.ch. Legal & Compliance entscheidet dann, ob die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem grossen Risiko für die Rechten und Freiheiten natürlicher Personen führen wird. Bejaht dies Legal & Compliance, so meldet es die Verletzung extern der zuständigen Aufsichtsbehörde (Art. 33 Abs. 1 DSGVO, Art. 24 DSG).

Die Meldung enthält mindestens folgende Informationen (Art. 33 Abs. 3 DSGVO, Art. 24 Abs 2 DSG)

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- Namen und Kontaktdaten der Anlaufstelle für weitere Informationen
- Beschreibung der wahrscheinlichen Folgen der Verletzung
- Beschreibung der ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung und gegebenenfalls Massnahmen zur Abmilderung von möglichen nachteiligen Auswirkungen

Hinweise dazu, wie Sie eine Datenschutzverletzung erkennen und melden, finden Sie in unserem **Verfahren und Schema zur Meldung bei Verletzungen des Schutzes personenbezogener Daten**.

Was du wissen musst

Eine **Datenschutz-Folgenabschätzung** oder **DSFA** ist:

Wenn ein neuer Verarbeitungsvorgang im Unternehmen verwendet wird (z. B. ein neuer E-Shop mit Zahlungsmöglichkeit, sodass neu Personendaten von Kunden, die online einkaufen, von uns verarbeitet werden), dann muss dieser Vorgang zunächst geprüft werden, nämlich ob er dem Zweck dient für den er erschaffen wurde (z. B. Verarbeiten von Adresse, Name, Bankinformation zur Online Zahlung mit Kreditkarte), ob er wirklich notwendig ist und verhältnismässig um diesen Zweck zu erreichen (z. B. benötige ich diese Information um die Kreditkarte zu belasten? Könnte ich die Kreditkarte auch mit weniger Information belasten?), ob sich neue potentielle Risiken für die Personendaten dadurch ergeben (z. B. könnte die Bankinformation durch einen externen Virenangriff gestohlen werden?) und wie man diese potentiellen Risiken mit welchen Massnahmen senken kann (z. B. benötige ich eine stärkere Firewall oder einen anderen Virenschutz damit ich die Sicherheit der Bankinformation garantieren kann?).

Eine **Meldung von Verletzungen des Schutzes von Personendaten** oder **Data Breach Notification** ist:

Falls unser Schutz verletzt wird (z. B. versehentliches Versenden einer Kundenliste mit persönlichen Daten an eine grössere externe Gruppe von Adressaten anstatt an eine bestimmte, hierzu bewilligte Person), dann ist dies sofort an Legal & Compliance über dataprotection@bmsuisse.ch zu melden. Es wird dann entschieden, ob die Verletzung zu einem grossen Risiko für die betroffenen Personen führt (z. B. waren viele Kunden auf dieser Liste? Waren die Daten besonders sensibel? Werden die Daten auf der Kundenliste nun potentiell von den unbewilligten Adressaten zum Versenden von Mailings benutzt oder an andere Unternehmen weiterverkauft?)

Eine Meldung an dataprotection@bmsuisse.ch muss mindestens folgende Informationen beinhalten:

- Beschreibung der Art der Verletzung (z. B. Kundenliste an x Personen versandt, es handelt sich um Kundendaten von x Kunden wie Name, Adresse, etc.)
- Beschreibung der wahrscheinlichen Folgen der Verletzung (z. B. die Kundendaten könnten nun für Verarbeitungen verwendet werden, für die sie ursprünglich nicht bestimmt warten und wir keine Einwilligung haben)
- Vorgeschlagene Massnahmen (z. B. wir könnten nun eine Mail an alle versenden und sie drauf hinweisen, dass sie diese Kundendaten löschen sollen/ nicht verwenden dürfen)

12. Compliance/ Reporting

Im Falle der Feststellung von ungenügender Konformität wird Legal & Compliance – im Zusammenhang mit dem betroffenen BMS Unternehmen – einen entsprechenden Prozess und Zeitplan definieren, um die Anforderungen in einem angemessenen und bestimmten Zeitraum zu erfüllen. Schwerwiegende Fälle werden der Geschäftsleitung gemeldet und von dieser gehandhabt.

13. Organisation

13.1 Geschäftsleitung

Die Geschäftsleitung definiert die übergeordneten Grundsätze für die Gewährleistung des Datenschutzes in den BMS Unternehmen. Sie ernennt ein zuständige Anlaufstelle die mit der Durchsetzung der datenschutzrechtlichen Vorgaben beauftragt wird.

13.2 Vorgesetzte

Die Vorgesetzten aller Stufen sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung der datenschutzrechtlichen Bestimmungen gemäss dieser Richtlinie verantwortlich. Sie sorgen in Zusammenarbeit mit der Anlaufstelle für Schulung und Sensibilisierung ihrer Mitarbeitenden. Sie nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, Massnahmen zum Datenschutz einzuhalten.

13.3 Zuständige Anlaufstelle

Legal & Compliance ist die von der Geschäftsleitung ernannte zuständige Anlaufstelle.

Legal & Compliance trägt die Dokumentenverantwortung für diese Datenschutzrichtlinie.

Die Data Protection Task Force (bestehend aus Mitarbeitenden der Abteilungen Legal & Compliance, IT und HR) unterstützt die BMS Unternehmen bei der Durchsetzung und Umsetzung des Datenschutzes.

Legal & Compliance beobachtet und berücksichtig die Entwicklung der gesetzlichen Vorgaben im Bereich des Datenschutzes

13.4 Alle anderen Mitarbeitenden

Alle Mitarbeitenden der BMS Unternehmen müssen die jeweils aktuellste Fassung dieser Datenschutzrichtlinie lesen und einhalten (auf BMSmobile unter dem internen ASTRA link erhältlich).

Wird festgestellt, dass Mitarbeitende mutwillig gegen diese Datenschutzrichtlinie verstossen haben, können Disziplinarmassnahmen bis hin zur Kündigung gegen diese eingeleitet werden.

13.5 Verantwortliche

13.5.1 Aussenverhältnis

Im Aussenverhältnis ist das jeweilige BMS Unternehmen Verantwortlicher.

Der Verantwortliche setzt insbesondere unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Massnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäss der DSGVO und dem DSG erfolgt.

13.5.2 Innenverhältnis

Der Leiter HR und die im HR tätigen Mitarbeitenden sind im Innenverhältnis für die sorgfältige und datenschutzkonforme Verarbeitung der personenbezogenen Daten für ihren Zuständigkeitsbereich verantwortlich.

Der Leiter IT trägt die Verantwortung im Innenverhältnis, dass die Datensicherheit und datenschutzrechtlichen Massnahmen technisch angemessen umgesetzt werden. Dabei unterstützen ihn insbesondere die Applikations- und Systemverantwortlichen. Er arbeitet eng mit Legal & Compliance zusammen, um die Konformität der Massnahmen zu prüfen. So beurteilt er Risiken, Vorfälle und Beinahe-Vorfälle, welche den Datenschutz gefährden können.

Was du wissen musst

Die **Geschäftsleitung** definiert die Datenschutzgrundsätze. Schwere Fälle von Datenschutzverletzungen sind der Geschäftsleitung zu melden.

Alle **Vorgesetzten** haben sich vorbildlich an die Grundsätze des Datenschutzes zu halten. Sie sorgen dafür, dass ihre Mitarbeitenden über diese Richtlinie und die Grundsätze des Datenschutzes informiert sind und wo nötig geschult werden.

Legal & Compliance ist die Anlaufstelle für Fragen, für das Führen des Verzeichnisses, für Aufnahmen von neuen Verarbeitungsvorgängen in das Verzeichnis, für das Erstellen von datenschutzrechtlichen Dokumenten, für Informations-, Auskunfts-, Berichtigungs-, Änderungs-, und Löschbegehren, für Meldungen bezüglich Datenschutzverletzungen und für alle anderen Sachverhalte rund um datenschutzrelevante Themen.

Alle Mitarbeitenden verpflichten sich mit Aufnahme der Arbeitsbeziehung mit einem BMS Unternehmen zur Befolgung dieser Datenschutzrichtlinie der BMS Unternehmen.

Nach **Aussen** treten die BMS Unternehmen als Datenschutzverantwortliche auf.

Intern sind vor allem Legal & Compliance, IT (für die technischen Massnahmen, das Durchführen von Datenschutz-Folgenabschätzungen und die Überprüfung von Verletzungsmeldungen) und HR (für besonders schützenswerte Personendaten und allgemein für Mitarbeitendendaten) zuständig, jedoch sind alle Mitarbeitenden zum Schutz von Personendaten verpflichtet.

14. Schlussbestimmungen

14.1 Änderungen und Ergänzungen

Diese Datenschutzrichtlinie kann schriftlich durch Legal & Compliance abgeändert, ergänzt oder aufgehoben werden. Als Änderung oder Ergänzung ist jegliche Hinzufügung, Streichung oder Modifikation einzelner Bestimmungen zu qualifizieren. Ausgenommen hiervon sind Berichtigungen formeller Art und von Flüchtigkeitsfehlern.

14.2 Ergänzende Dokumente

Diese Datenschutzrichtlinie stellt die Grundlage für die datenschutzrechtlichen Vorgaben der BMS Unternehmen dar. Abgeleitet von dieser können Weisungen und weitere Dokumente erarbeitet werden, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten notwendig sind.

14.3 Integrierende Bestandteile

Folgende Anhänge bilden Bestandteile dieser Datenschutzrichtlinie:

1: Prozessablauf für Auskunfts-, Korrektur- und Löschungsanfragen

2: Auskunftsbegehren intern

3: Auskunftsbegehren extern

4: Korrekturbegehren intern

5: Korrekturbegehren extern

6: Löschungsbegehren intern

7: Löschungsbegehren extern

8: Konzept Datenschutz-Folgenabschätzung

9: Verfahren & Schema Data Breach Notification

14.4 Diverses

Diese Datenschutzrichtlinie ist allen Mitarbeitenden zugänglich über BMSmobile.

Legal & Compliance trägt die Dokumentenverantwortung für diese Datenschutzrichtlinie. Alle Fragen in diesem Zusammenhang sind via E-Mail an dataprotection@bmsuisse.ch zu senden.

Relevante Änderungen oder Ergänzungen zu dieser Datenschutzrichtlinie werden den Mitarbeitenden der BMS Unternehmen durch HR mitgeteilt. Sie treten im Moment der Publizierung auf BMSmo-bile in Kraft.

14.5 Inkrafttreten

Diese Datenschutzrichtlinie tritt in Kraft ab September 2022.