VERFAHREN BEI VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

1. EINFÜHRUNG

Bei Verletzung oder mutmasslicher Verletzung des Schutzes personenbezogener Daten gelangt das vorliegende Verfahren zur Anwendung. Mit diesem Verfahren soll sichergestellt werden, dass die BMS Unternehmen jegliche Verletzungen des Schutzes personenbezogener Daten (wie nachstehend definiert) schnell bearbeiten und möglichst eingrenzen können.

WAS SIND PERSONENBEZOGENE DATEN?

Als **personenbezogene Daten** werden alle Informationen bezeichnet, die eine lebende natürliche Person betreffen und eine Identifizierung dieser Person ermöglichen. Eine Person ist identifizierbar, wenn sich durch die Daten ohne allzu grossen Aufwand Rückschlüsse auf ihre Identität ziehen lassen. Beispiele für personenbezogene Daten sind: Name, Anschrift, Geburtsdatum, Telefonnummer, Kontonummer, Berufsbezeichnung, Foto, usw.

2. WAS IST EINE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN?

Definition:

Der Schutz der Datensicherheit ist verletzt, wenn Personendaten, egal ob unbeabsichtigt oder widerrechtlich, ob durch ein Handeln/Unterlassen von Dritten oder Mitarbeitenden/Partnern verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Beispiele:

Verlust oder Diebstahl eines Laptops oder Mobiltelefons mit personenbezogenen Daten, Senden einer (ungeschützten) Excel-Datei usw. mit personenbezogenen Daten an eine unbefugte Person, Drucken von Gehaltsangaben und Zurücklassen dieser Ausdrucke am Drucker, Hacken eines Systems, das personenbezogene Daten enthält und/oder Verlust bzw. Diebstahl von Dateien usw.

Es liegt hingegen keine Verletzung vor, wenn bei einem Verlust bzw. Beeinträchtigung

(i) die personenbezogenen Daten verschlüsselt oder anonymisiert sind,

(ii) es eine vollständige, aktuelle Sicherung der personenbezogenen Daten gibt und

(iii) der Zugriff auf die personenbezogenen Daten überwacht wird.

Dementsprechend muss im Einzelfall geprüft werden, ob ein Datenschutzvorfall eine Verletzung des Schutzes personenbezogener Daten ist.

3. WANN KOMMT DAS VERFAHREN ZUR ANWENDUNG?

Wenn an einem Datenschutzvorfall personenbezogene Daten beteiligt sind und diese nicht verschlüsselt oder anonymisiert und vollständig gesichert sind und wenn der Zugriff auf die Daten nicht überwacht wird, liegt womöglich eine Verletzung des Schutzes personenbezogener Daten vor und das untenstehende Verfahren kommt zur Anwendung.

4. WIE WIRD EINE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN INTERN GEMELDET?

4.1 Erste Meldung

Sobald Sie Kenntnis von einer tatsächlichen oder mutmasslichen Verletzung des Schutzes personenbezogener Daten erlangen, melden Sie dies sofort den Abteilungen **Legal & Compliance** und **IT** per E-Mail an **dataprotection@bmsuisse.ch** und **helpdesk@bmsuisse.ch**.

Zunächst prüfen die Abteilungen Legal & Compliance und IT, ob es sich um eine Verletzung des Schutzes personenbezogener Daten handelt.

4.2 Massnahmen

Hat eine Verletzung des Schutzes personenbezogener Daten stattgefunden, sind unter Leitung der Abteilung Legal & Compliance, mit dem Direktor der von der Verletzung betroffenen Abteilung und mit der Abteilung IT die nachfolgenden Punkte zu klären.

- Kategorie und Anzahl der betroffenen Daten,
- Bestimmen der notwendigen Massnahmen, die unverzüglich zur Begrenzung der Verletzung ergriffen werden müssen,
- Klären, ob der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB oder allenfalls die betroffenen Personen selbst über die Verletzung informiert werden müssen,
- Bestimmen der potenziellen Konsequenzen für das Unternehmen und die betroffenen Personen,
- Haftungsfragen Dritter klären,
- Angemessene Massnahmen für die Zukunft bestimmen.

4.3 Benachrichtigung des EDÖB erforderlich?

Nicht jede Verletzung des Schutzes personenbezogener Daten muss dem EDÖB gemeldet werden, sondern nur Verletzungen mit einem «hohen Risiko» negativer Folgen für die betroffenen Personen. Verletzungsvorfälle bedürfen also einer Überprüfung durch die Abteilung Legal & Compliance, welche dann nach Bedarf (und nach Rücksprache mit dem MD) Meldung an die zuständige DSB erstattet.

4.4 Mitteilung an die betroffenen Personen erforderlich?

Eine Mitteilung an die betroffenen Personen muss nur gemacht werden, falls es zu ihrem Schutz erforderlich ist, also falls sie zB ein Passwort ändern müssen, damit der verletzte Schutz eines Online-Kontos wiederhergestellt ist, weil die Zugangsdaten durch Unberechtigte abgegriffen wurden.

5. WAS MUSS DEM EDÖB GEMELDET WERDEN?

Fall eine Meldung an das EDÖB getätigt werden muss, hat diese so rasch als möglich zu erfolgen und muss mindestens folgende Angaben enthalten:

- **Art der Verletzung** der Datensicherheit,
- **wahrscheinliche Konsequenzen**, die aufgrund der Verletzung des Schutzes personenbezogener Daten zu erwarten sind,
- **ergriffene oder geplante Massnahmen zur Behebung der Verletzung** des Schutzes personenbezogener Daten.

Falls Sie Fragen haben oder weitere Hilfestellung benötigen, wenden Sie sich dataprotection@bmsuisse.ch

Schema - **Verfahren bei Verletzung des Schutzes personenbezogener Daten**