Durchführung einer Datenschutz-Folgenabschätzung (DSFA)

Abteilung: Legal & Compliance

Verfasser: Hooker Christina, Legal Counsel

Erstellt: Bern, 12.09.2022

Kurzkonzept
Die BMS Building Materials Suisse (**BMS**) nimmt den Schutz personenbezogener Daten und das Befolgen der relevanten Datenschutzgesetze sehr ernst. Unter anderem bedeutet dies, dass BMS der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, allgemein als Datenschutz-Grundverordnung (**DSGVO**) bekannt und dem Schweizer Datenschutzgesetz (**DSG**) untersteht, da die Muttergesellschaft BME ihren Sitz in den Niederlanden hat während BMS in der Schweiz sitzt und agiert. Dies zieht Pflichten für BMS mit sich. Das Durchführen von Datenschutz-Folgenabschätzungen (**DSFA**) bei neu geplanten Verarbeitungstätigkeiten von personenbezogenen Daten, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, ist gemäss Artikel 35 DSGVO und Art. 20 f DSG eine solche Pflicht, welche der BMS als Verantwortliche obliegt. BMS übergibt die eigentliche Durchführung der Datenschutz-Folgenabschätzungen und alle damit zusammenhängenden Befugnisse den Departementen Legal & Compliance und IT, ist sich jedoch Ihrer unveränderten Verantwortung bewusst.

Eine Datenschutz-Folgenabschätzung ist ein Verfahren, anhand dessen die zu untersuchende Verarbeitung beschrieben, ihre Notwendigkeit und Verhältnismässigkeit bewertet und die Risiken für die Rechte und Freiheiten natürlicher Personen, die die Verarbeitung personenbezogener Daten mit sich bringt, durch eine entsprechende Risikoabschätzung und die Ermittlung von Abhilfemassnahmen besser kontrolliert werden sollen. Eine Datenschutz-Folgenabschätzung ist also ein Verfahren zur Sicherstellung und zum Nachweis der Einhaltung gesetzlicher Anforderungen.
Dieses Kurzkonzept stellt die notwendigen Schritte für die Erstellung eines nachhaltigen Prüf – und Nachweisverfahrens dar:

Schritt 1: Verarbeitungstätigkeitsverzeichnis

Das Verzeichnis der bestehenden Verarbeitungstätigkeiten der BMS kann nur durch Legal & Compliance eingesehen und angepasst werden und ist entsprechend durch angemessene technische und organisatorische Massnahmen zu schützen.

Sollten im Rahmen neuer Produkte, neuer Projekte oder bei der Verwendung neuer Technologien noch nicht bei BMS bestehende Verarbeitungstätigkeiten entstehen, so sind diese von der für das Produkt, Projekt oder für die neue Technologie zuständigen Person (**Zuständige Person**) per mail an dataprotection@bmsuisse.ch zu melden.

Schritt 2: Eine Risikobeurteilung für die neu gemeldeten Verarbeitungstätigkeiten erstellen

Wenn Legal & Compliance nach einer ersten kurzen Überprüfung der neu gemeldeten Verarbeitungstätigkeit mittels der Checkliste «Risikobeurteilung Verarbeitungstätigkeiten» (nicht öffentlich hinterlegt) entscheiden, dass eine DSFA durchgeführt werden soll, dann rufen sie

hierzu die Data Protection Task Force (**DP Task Force**) zusammen. Die DP Task Force setzt sich aus ausgewählten Mitgliedern aus Legal & Compliance, IT, HR und der Zuständigen Person zusammen.

Die ausgefüllten Checklisten dienen dem Nachweis der Überprüfung der Notwendigkeit einer DSFA und sind, ungeachtet des Resultats, von Legal & Compliance sicher aufzubewahren.

Schritt 3: Wo notwendig, Durchführung einer Datenschutz-Folgenabschätzung

Bestimmt Legal & Compliance hingegen, dass eine DSFA erforderlich ist, so dokumentieren sie ihren Entscheid ebenfalls mit der obigen Checkliste, informieren die Zuständige Person darüber, dass die Weiterführung der geprüften Verarbeitungstätigkeit (des neuen Verfahrens/der neuen Dienstleistung/ der neuen App/ des neuen System/etc) bis auf Weiteres sistiert ist und rufen die DP Task Force zusammen um die DSFA durchzuführen.

Die Zuständige Person muss die Weiterführung der entsprechenden Verarbeitungstätigkeit (des neuen Verfahrens/der neuen Dienstleistung/ der neuen App/des neuen Systems/etc) bis zum Resultat der DSFA sistieren.

Legal & Compliance leitet nun mit der DP Task Force das Datenschutz-Folgenabschätzungsverfahren gemäss dem Leitfaden zur Durchführung einer Datenschutz-Folgenabschätzung (nicht öffentlich hinterlegt) ein.

Die DP Task Force hat nun einen Zeitrahmen von vierzehn (14) Arbeitstagen (eine Verlängerung des Zeitrahmens liegt im Ermessen von Legal & Compliance, muss aber begründet werden können), um die DSFA durchzuführen und geeignete Abhilfemassnahmen zu erörtern.

Schritt 4: Regelmässige Überprüfung

Es obliegt der DP Task Force, die Datenschutz-Folgenabschätzungen

A) **Alle drei (3) Jahre** zu überprüfen

oder

B) **Immer dann, wenn** hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risiken **Änderungen** eintreten