TALOS

Publikation

Der Data Protection Officer (DPO) - die neue Compliance Schlüsselfigur

von Martin Bonnet

Die Funktion des Data Protection Officer (DPO) gewinnt aktuell stetig an Bedeutung. Während Rolle und Verantwortlichkeiten in der Vergangenheit weitgehend undefiniert waren, legt nun die EU DSGVO die erforderlichen Qualitäten und Aufgaben eines DPO genau fest.

Die Funktion des DPO ist für die Wahrung des Datenschutzes innerhalb einer Organisation nunmehr von entscheidender Bedeutung.

Dieser Artikel zeigt eingangs die Notwendigkeit eines DPO für Unternehmen auf und erläutert die Rolle und Stellung eines DPO innerhalb einer Unternehmung. Anhand zwei konkreter Beispiele wird schliesslich aufgezeigt, wie der DPO in die Prozesse der Organisation einzugliedern ist, damit er seinen Pflichten im Sinne der Verordnung stets nachkommen kann.

Publikation

Braucht mein Unternehmen einen DPO?

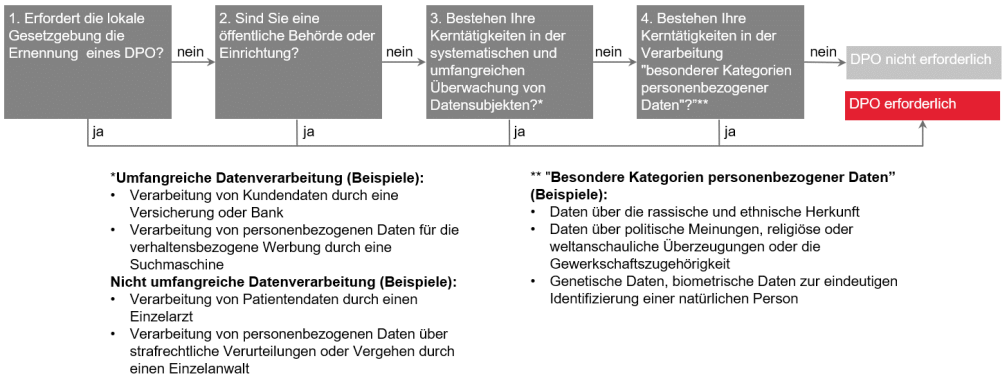

Abbildung:
Notwendigkeit eines DPO
(Quelle: Eigene Darstellung)

Wird ein DPO benötigt, bleibt dem Unternehmen freigestellt, ob die Position des DPO intern oder extern besetzt wird. Insbesondere für kleinere Unternehmen ist es von Vorteil, einen externen Datenschutzbeauftragten zu bestellen, um die eigenen (internen) Ressourcen besser nutzen zu können und die Vorteile des spezifischen Fachwissens eines externen DPO zu erhalten. Für international tätige Unternehmen ermöglicht die Verordnung die Ernennung eines konzernübergreifenden DPO, „sofern der DPO für jede Niederlassung ohne Umstände kontaktiert werden kann". In der Praxis wird in der Regel ein DPO pro Niederlassung bzw. Tochtergesellschaft bestellt, um eine bessere Verfügbarkeit durch die lokale Datenschutzbehörde zu gewährleisten.

Braucht mein Unternehmen einen DPO?

Die untenstehende Darstellung fasst die Anforderungen und Merkmale des DPO zusammen und zeigt auf, welchen Mehrwert seine weitreichende Verantwortung und seine zentrale Position für die Organisation bieten.

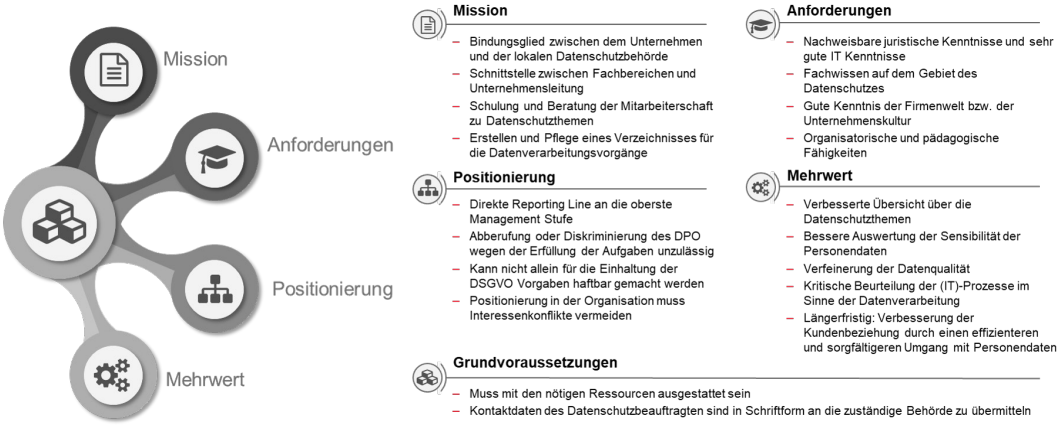

Abbildung:
Rolle eines DPO
(Quelle: Eigene Darstellung)

TALOS

Publikation

Case Study 1 – Durchführung eines DPIA (Data Privacy Impact Assessment)

Bei einem DPIA ist zu prüfen, ob und in welchem Ausmass eine (beabsichtigte) Verarbeitung von personenbezogenen Daten Auswirkungen und Risiken für die Rechte und Freiheiten von natürlichen Personen zur Folge hat. Obwohl der DPO nicht selber für die Durchführung eines DPIA zuständig ist, prüft er, ob ein solches Verfahren notwendig ist und stellt sicher, dass dieses ggf. ordnungsgemäss durchgeführt wird (Überwachungsrolle). Die folgenden Schritte werden beachtet:

1. Auswertung des Bedarfs eines DPIA

Eine Organisation muss eine Datenschutz-Folgeabschätzung (DPIA) durchführen, wenn die Verarbeitung von personenbezogenen Daten ein hohes Risiko darstellt.

Dies ist der Fall, wenn die Verarbeitung:

- Als Grundlage für Entscheidungen dient, die Rechtswirkungen gegenüber natürlichen Personen haben oder diese in erheblicher Weise beeinträchtigen können (z.B. bei Bonitätsprüfungen).
- Eine umfangreiche Aufarbeitung besonderer Kategorien personenbezogener Daten („sensitive data“) oder strafrechtlich relevante Daten umfasst.
- Die Durchführung einer systematischen und umfangreichen Überwachung öffentlicher Bereiche umfasst.

Falls sich herausstellt, dass die beabsichtige Datenverarbeitung ein DPIA erfordert, muss umgehend eine Meldung an die zuständige Behörde durch den DPO erfolgen.

2. Bewertung der Verarbeitungsvorgänge

Geplante Verarbeitungsvorgänge werden durch den verantwortlichen Fachbereich systematisch beschrieben. Verarbeitungsvorgänge werden daraufhin durch den DPO auf folgende Aspekte hin überprüft, welche im Art. 5 der EU DSGVO festgehalten werden:

- Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz: alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten müssen leicht zugänglich und verständlich in klarer Sprache formuliert sein.
- Zweckbindung: personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen ausschliesslich in einer mit diesen Zwecken zu vereinbarenden Weise weiterverarbeitet werden.
- Datenminimierung: personenbezogene Daten müssen auf das für die Zwecke der Verarbeitung notwendige Mass beschränkt sein.
- Richtigkeit: personenbezogene Daten müssen sachlich richtig und auf dem neusten Stand sein.

3. Risikobewertung

Die Risiken für die Rechte und Freiheiten der betroffenen Personen werden anhand folgender Kriterien bewertet:

- Wahrscheinlichkeit: wie hoch ist die Wahrscheinlichkeit, dass ein Datenmissbrauch (z.B. Datenleck) eintritt?
- Schweregrad: welche Konsequenzen hat ein Datenmissbrauch auf das Privatleben, die Grundrechte und/oder die finanzielle Situation einer natürlichen Person?

4. Bestimmung der Abhilfemassnahmen

Nach der Risikobewertung werden Abhilfemassnahmen (z.B. Garantien, Sicherheitsvorkehrungen und Verfahren, Anspruch auf Datenlöschung durch Betroffenen) erarbeitet, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden kann, dass die Bestimmungen der EU DSGVO eingehalten werden.

5. Festlegung und Mitteilung der Ergebnisse

Zum Schluss werden die Ergebnisse des DPIA den betreffenden Parteien durch den DPO mitgeteilt. Die Behörde, bei der zu Beginn das Verfahren gemeldet wird, gibt innerhalb von 8 Wochen eine Empfehlung, falls sie der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit der EU DSVGO steht. Es ist aber keine explizite Genehmigung der Behörde zu erwarten.

Case Study 2 – Lieferanten-Management

Die Vorgaben der EU DSGVO gelten nicht nur für interne Datenverarbeitungsvorgänge, sondern auch für Auftragsdatenverarbeitungen (ADV), bei welchen Lieferanten für die Verarbeitung von personenbezogenen Daten im Auftrag einer Unternehmung herangezogen werden.
In solchen Fällen muss eine Datenschutz-Auswertung stattfinden, bevor der Vertrag abgeschlossen werden kann.

Diese Auswertung erfolgt in der Regel durch einen Fragebogen, der folgende Fragen beinhaltet:

- *Um was für eine Dienstleistung handelt es sich, wie lange soll die Dienstleistung andauern?*
- *Wozu dient die Dienstleistung, welches Ziel soll erreicht werden und mit welchen Mitteln?*
- *Welche Daten oder Datenkategorien werden verarbeitet, erhoben oder genutzt?*
- *Wessen personenbezogene Daten werden verarbeitet (z.B. Mitarbeiter oder Kunden des Auftraggebers)?*
- *Verfügt der Auftragnehmer über die nötigen Datenschutzzertifizierungen?*
- *Hat der Auftragnehmer eine Weisung zur Einhaltung der Datenschutzvorgaben umgesetzt?*

Der DPO gibt in diesem Zusammenhang eine Empfehlung auf Basis der Ergebnisse des Fragebogens ab, welcher vom Bedarfsträger (ggf. nach Rücksprache mit dem potentiellen Lieferanten) ausgefüllt wird. Diese Empfehlung ist nicht bindend. Folgt jedoch der Bedarfsträger nicht der Empfehlung durch den DPO, trägt er bzw. sein Fachbereich die volle Verantwortung im Falle eines entstehenden Datenmissbrauchs. Der Vorgang lässt sich wie folgt zusammenfassen:

Abbildung:
GDPR Auswertung beim Lieferanten-Onboarding
(Quelle: Eigene Darstellung)

Ausblick

Die Ernennung eines DPO sollte nicht nur als notwendiges Übel auf dem Weg zur Compliance mit der EU DSGVO betrachtet werden. Als Anlaufstelle der Datenschutzbehörde innerhalb einer Organisation und Garant für die Einhaltung der EU DSGVO Vorgaben spielt der DPO eine zentrale Rolle, die längerfristig einen effizienteren und rechtskonformen Umgang mit personenbezogenen Daten ermöglichen soll. Wie sich diese Rolle konkret etablieren lässt und welchen tatsächlichen Mehrwert der DPO für die Wahrung des Datenschutzes bringen wird, kann noch nicht abschliessend beurteilt werden.

Wir bei TALOS sind davon überzeugt, dass die Funktion des DPO weiterhin an Bedeutung gewinnen wird (ähnlich zu den Risk und Compliance Abteilungen nach der Finanzkrise). Wir wissen welche Herausforderungen die Etablierung eines DPO und die laufende Einhaltung der EU DSGVO Vorgaben in Ihrer Organisation mit sich bringen. Dank unserer erprobten „Operating Model Transformation“ Expertise und unserer langjährigen Projekterfahrung bei der Implementierung regulatorischer Auflagen können wir Sie unter anderem bei einem GDPR Readiness Assessment unterstützen und helfen Lücken und Risiken zu identifizieren und zu schliessen. Für die laufende Überwachung der Erfüllung von Compliance-Anforderungen unterstützen wir bei dem Aufbau eines Kontroll- und Überwachungssystems.

Publikation

Wer wird sind

TALOS definiert neue Standards in der Management Beratung. Als spezialisierte Boutique Beratung mit Schweizer Wurzeln und Büros in Zürich und Luxembourg beraten wir Kunden aus der Europäischen Finanzindustrie.

TALOS wurde 2008 von erfahrenen Management Beratern gegründet und ist seither zu einem etablierten Beratungsunternehmen für Finanzunternehmen gewachsen. **2018 feiern wir unser 10-jähriges Jubiläum.**

Als Experten für regulatorische Transformationslösungen decken wir die gesamte Bandbreite möglicher Fragestellungen ab, von der Analyse über die Strategie bis hin zur Umsetzung.

Zürich
TALOS Management Consultants
Bleicherweg 45
CH-8002 Zürich

Luxembourg
TALOS Management Consultants
5, Rue Heienhaff | 2nd floor (Wing E – Suite 2E)
L-1736, Senningerberg

Ihr Kontakt

Christian ist Partner bei TALOS und begann seine Karriere als Berater bei einem Deutschen Logistikkonzern. Nach langjähriger Tätigkeit als Management-Consultant bei Accenture stiess er 2008 zu TALOS und verantwortet bei uns den Bereich Risk & Compliance.

Christian Scholten
Partner
Risk & Compliance
+41 44 380 14 40
christian.scholten@talos-consultants.ch

Martin Bonnet
Senior Consultant
+41 44 380 14 40
martin.bonnet@talos-consultants.ch