PRIVACYDESK®
SUISSE

DER DPO IN DER PRAXIS UND DIE ORGANISATION DIESER FUNKTION

EINLEITUNG

WER IST DAS DPO

Die Figur des DPOs ist **nicht neu** und hat sich im Laufe der Jahre zu einer weltweit verbreiteten Praxis entwickelt:

- Hessischen Datenschutzgesetz (HDSG) of 1970 - DE
- Richtlinie 95/46/EC - EU
- Verordnung (EU) 2016/679 (GDPR) - EU
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) - USA
- Personal Information Protection Law of 2021 (PIPL) - PRC

WER IST DER DPO

In der Schweiz werden die Figur des DPOs und seine Aufgaben werden geregelt durch:

Art.10 nDSG

Art. 23 Verordnung über den Datenschutz
(nachstehend ‘DSV')

WER IST DER DPO

- Der Datenschutzberater (DSB) oder „Data Protection Officer“ (DPO) ist eine Berufsbezeichnung, die in der Schweiz mit dem am 1. September 2023 in Kraft tretenden neuen **Bundesgesetz**
- **über den Datenschutz** (nachstehend „nDSG") eingeführt wurde.

- Der DPO ist eine professionelle Stelle, die mit einer Unternehmensfunktion (sowohl intern als auch extern) betraut ist und über Kenntnisse in den Bereichen **Recht, IT, Risikomanagement und Prozessanalyse verfügt**.

- Seine Hauptaufgabe besteht darin, die Verwaltung der Personendaten (und damit deren Schutz) für das Unternehmen **zu überwachen, zu bewerten und zu organisieren**, so dass sie im Einklang mit dem geltenden Datenschutzrecht behandelt werden.

DPO: AUFGABEN UND EIGENSCHAFTEN

DPO: AUFGABEN

Bietet Schulungen und Beratung für das Unternehmen in Bezug auf den Datenschutz an

Beteiligt sich an der tatsächlichen Umsetzung des Datenschutzrechts im Unternehmen

Dient als Ansprechpartner für die betroffenen Personen und die für den Datenschutz zuständigen Behörden

Bewertet die Bearbeitung von Personendaten und bietet Korrekturmassnahmen an, um Verstösse gegen das Datenschutzrecht zu vermeiden

Beteiligt sich an der Ausarbeitung und Überprüfung von Datenschutz-Folgenabschätzungen (DSFA)

DPO: EIGENSHAFTEN

Unabhängigkeit und Selbstständigkeit

- Keine Interessenkonflikte
- Die Funktion des DPOs ist eine unabhängige Funktion, die von anderen bestehenden Aufgaben/Rollen der ernannten Person getrennt ist
- Reservierte Zeit und Budget für die Ausübung der Funktion
- Der DPO ist direkt der obersten Führungsebene unterstellt

Einbindung

- Der DPO muss frühzeitig und in angemessener Weise in alle Datenschutzfragen einbezogen werden
- Regelmässige Treffen zwischen dem DPO und der obersten Führungsebene, dem Privacy Manager, dem Legal & Compliance Manager sowie anderen internen Unternehmensfunktionen mit Auswirkungen auf das Datenschutzrisiko können vereinbart werden

Hilfe

- Erleichtert den Behördenvertretern den Zugriff auf die richtigen und notwendigen Dokumente und Informationen
- Schnittstelle zur Geschäftsleitung und Erleichterung der Auslegung und Anwendung der Datenschutzbestimmungen im Unternehmen

Fristgerechte Meldung

- Eine rechtzeitige Mitteilung der genauen und aktuellen Kontaktdaten des DPOs an die Behörde ist erforderlich
- Die Kontaktdaten des DPOs müssen intern im Unternehmen bekannt gegeben werden und in Datenschutzdokumenten wie Datenschutzhinweisen und Aufzeichnungen über Datenverarbeitungstätigkeiten erscheinen

DER DPO UND DAS UNTERNEHMEN

DER DPO UND DAS UNTERNEHMEN

- Der DPO kann, muss aber nicht, durch einen Arbeitsvertrag an das Unternehmen gebunden sein.

- Der DPO kann ein Angestellter des Unternehmens oder ein externer Berater sein, aber in beiden Fällen muss die Tätigkeit unabhängig von den anderen Aufgaben und Tätigkeiten, die bereits für das Unternehmen ausgeführt werden, ausgeübt werden.

- Darüber hinaus empfiehlt der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, dass die Rolle des DPOs von anderen Arten der Beratung (z.B. Privacy Consultant, Rechtsberater) und von der rechtlichen Vertretung desselben Unternehmens (z.B. CEO) getrennt sein sollte

WIE WIRD DER DPO ERNANNT

Wird ein interner Mitarbeiter gewählt, so muss die Ernennung zum "Datenschutzberater" formalisiert werden.

Wird hingegen eine externe Person ausgewählt, so ist diese Ernennung Bestandteil eines Dienstleistungsvertrags

FEHLER ZU VERMEIDEN

Bei der Auswahl eines DPO:

- Die Ernennung als reine Formalität zu betrachten
- Das Streben nach maximalen Einsparungen zum Nachteil des Dienstes (insbesondere bei externen DPOs)
- Eine nicht unabhängige Person mit einem Interessenkonflikt zu wählen

Wichtige praktische Lösungen:

- Formalisierung der für die Tätigkeit des DPOs zugewiesenen Zeit und derjenigen, die für andere Aufgaben im Büro zugewiesen wird
- Bereitstellung eines Weiterbildungsbudgets für kontinuierliche Schulungen (für interne DPOs)
- Sicherstellung der erforderlichen unterstützenden Mittel

VOR- UND NACHTEILE

Kein einheitlicher Ansatz | flexibel je nach Situation

	Internes DPO	Externes DPO
+	Umfassende Kenntnisse über das Unternehmen Einfluss (zur Durchsetzung des Datenschutzes im Unternehmen)	Weniger Probleme mit der Unabhängigkeit Erfahrung im Umgang mit dem EDÖB Spezialisierte Kenntnisse im Bereich des Datenschutzes
-	Mögliche Interessenkonflikte Kosten Suche nach dem richtigen Kandidaten	Geringere Kenntnisse der Organisation/des Sektors Geringere Präsenz in der Organisation (zeitliche Verfügbarkeit)

EIN TEAM FÜR DEN DPO?

EIN TEAM FÜR DAS DPO

Personen, die Fähigkeiten der Einzelnen und ihre Stärken können so kombiniert werden, dass verschiedene Personen, die in einem TEAM arbeiten, die verschiedenen Aufgaben effektiver erfüllen können

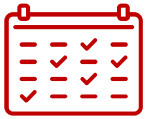
Es ist empfohlen, eine **klare Aufgabenteilung** innerhalb des DPO-Teams vorzunehmen und dem DPO die Rolle des "Ansprechpartners/Teamleiters" in dem Unternehmen zuzuweisen.

Es wäre **hilfreich**, diese Punkte im Rahmen des Dienstleistungsvertrags festzulegen.

DIE TÄTIGKEIT DES DPOs

DPO-UNTERLAGEN

Regulierung der Erbringung der Dienstleistung des DPOs



DPO Überwachungs- und Tätigkeitsplan

Berichte und Protokolle

Jede DPO-Sitzung muss ein spezielles Protokoll mit Angabe der durchgeführten Kontrollen, kritischen Punkte und Konformitäten erstellen.

Ein jährlicher Bericht an die oberste Führungsebene sollte vorgelegt werden, in dem die Ergebnisse der vorgenannten Sitzungen und Kontrollen erläutert werden.

REGULIERUNG DER ERBRINGUNG DER DIENSTLEISTUNG DES DPOs

Der DPO, ob intern oder extern, entwirft die Regulierung der Dienstleistung, welche beschreibt:

- Die Aufgaben des DPOs
- Die Zusammensetzung des DPOs (einzeln oder im Team)
- Die Modalitäten für die Planung der Tätigkeit (z.B. Häufigkeit der Sitzungen, Einberufungsmodalitäten, Festlegung des Arbeitsortes, Bereitstellung von Protokollen/Berichten)
- Wie werden Protokolle/Berichte aufbewahrt und zugänglich gemacht?
- Wie werden Dokumente/Abläufe aufbewahrt und zugänglich gemacht?
- Die Art und Weise, wie Überprüfungen/Einsätze durchgeführt werden (z.B. Verweis auf den Aktivitätsplan, Durchführung geplanter Kontrollen oder auf Wunsch des Unternehmens)

REGULIERUNG DER ERBRINGUNG DER DIENSTLEISTUNG DES DPOs

Der DPO, ob intern oder extern, entwirft die Regulierung der Dienstleistung, welche beschreibt:

- Die Hypothesen und Modalitäten für die Einbeziehung externer Parteien
- Die ausgewiesenen materiellen und finanziellen Ressourcen (ohne Angabe des Umfangs, aber mit Verweis auf den Dienstleistungsvertrag), einschliesslich der Angabe eventueller zusätzlicher Kosten für Reisen/Audits
- Die Berichterstattungsmethoden des DPOs (z.B. vertrauliche E-Mails, Stellungnahmen, Protokolle/Berichte, Vorladungen der Geschäfts-führung, regelmässige Berichte)
- Vertraulichkeitsklausel
- Modalitäten für die Änderung der Regulierung

REGULIERUNG DER ERBRINGUNG DER DIENSTLEISTUNG DES DPOs

Der DPO, ob intern oder extern, entwirft die Regulierung der Dienstleistung, welche beschreibt:

- Verantwortungselemente (z. B. Schulung/Information des Personals, Corporate Governance [Vollmachten, Vollmachten usw.], Ergreifung technischer Sicherheitsmaßnahmen)
- Dokumentationsmanagement der Dienstleistung des DPOs (ordnungsgemässe Archivierung der Protokolle des DPOs und ihrer Anhänge)
- Die Art und Weise, wie Interviews mit der Geschäftsleitung/den Bereichsvertretern geführt werden
- Die Möglichkeit, Stellung zu Datenschutzfolgenabschätzungen zu nehmen und deren ordnungsgemässe Durchführung zu überwachen

REGULIERUNG DER ERBRINGUNG DER DIENSTLEISTUNG DES DPOs

Der DPO, ob intern oder extern, entwirft die Regulierung der Dienstleistung, welche beschreibt:

- Standard-Informationsflüsse an den DPO (z.B. bei Datenschutz-verletzungen, Anfragen der betroffenen Personen, Anfragen der Behörde usw.)
- Regelmässiger Informationsfluss vom DPO zum Management (z.B. halbjährlicher/jährlicher Bericht über die Tätigkeit des DPOs)
- Zu prüfende Unterlagen (z.B. Datenschutzhinweise, Risikobewertung)
- Überprüfung in Bezug auf die Erstellung und Aktualisierung des Verzeichnisses der Bearbeitungstätigkeiten;

DER DPO IM ÖFFENTLICHEN BEREICH

DER DPO IM ÖFFENTLICHEN SEKTOR

Jedes Bundesorgan ernennt einen DPO.

Mehrere Bundesorgane können gemeinsam einen Datenschutzbeauftragten ernennen.

Es gelten die gleichen Pflichten und Vorgaben wie im privaten Sektor

(z.B. Zugang, Unabhängigkeit und Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten im Internet und Meldung an den EDÖB)

DPO
=
WHISTLEBLOWER?

DPO=WHISTLEBLOWER?

Ist es denkbar, dass der DPO verpflichtet ist, die Behörde zu informieren, wenn der für die Verarbeitung Verantwortliche gegen die Datenschutzvorschriften verstösst und eine Straftat begeht?

Der DPO ist nicht der Whistleblower der Datenschutzbehörde!

PRIVACYDESK®
SUISSE

VIELEN DANK!

Gianfranco Valsecchi

privacydesk.ch

info@privacydesk.ch