PRIVACYDESK®
SUISSE

LE DPO EN PRATIQUE ET COMMENT ORGANISER CETTE FONCTION

INTRODUCTION

QUI EST LE DPO

La figure du DPD **n'est pas** nouvelle et est devenue une pratique courante à l'échelle mondiale au fil des ans :

- LPD de la Hesse (HDSG) de 1970 - DE
- Directive 95/46/CE - UE
- Règlement (UE) 2016/679 (GDPR) - UE
- Loi de 1996 sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) - États-Unis
- Loi sur la protection des informations personnelles de 2021 (PIPL) - RPC

QUI EST LE DPO

En Suisse, la figure du DPO et ses fonctions sont assurées par:

Art.10 nLPD

L'art. 23 de l'Ordonnance sur la protection des données (ci-après dénommée "OPDo")

QUI EST LE DPO

- Data Protection Advisor (DPA) or Data Protection Officer (DPO) est un professionnel introduit, en Suisse, par la nouvelle **loi fédérale sur la protection des données** (ci-après «nLPD"), qui entrera en vigueur à partir du 1er septembre, 2023.

- Le DPO est un professionnel nommé pour jouer un rôle au sein d'une entreprise (interne ou externe) et **possédant des compétences juridiques, informatiques, de gestion des risques et d'analyse des processus.**

- Sa principale responsabilité est de **surveiller, d'évaluer et d'organiser** la gestion des données personnelles (et donc leur protection) pour l'entreprise, de manière à ce qu'elles soient traitées conformément à la législation applicable en matière de protection de la vie privée.

FONCTIONS ET CARACTÉRISTIQUES DES DPO

FONCTIONS DU DPO

Fournit des formations et des conseils à l'entreprise en ce qui concerne la protection des données.

Participe à l'application concrète droit de la vie privée au sein de l'entreprise

sert de point de contact pour les personnes concernées et pour les autorités compétentes en matière de protection des données

évalue le traitement des données personnelles et propose des mesures correctives pour éviter les violations droit de la vie privée

Participe à l'élaboration et à la vérification des analyses d'impact relatives à la protection des données (AIPD)

CARACTÉRISTIQUES DU DPO

Indépendance et autonomie

- Pas de conflits d'intérêts
- La fonction de DPO est un travail indépendant, distinct des autres tâches/rôles que la personne désignée peut déjà avoir.
- Temps et budget consacrés à l'exercice de la fonction de DPD
- Le DPD rend compte directement à la direction générale

Implication

- Le DPO doit être impliqué rapidement et de manière adéquate dans toutes les questions relatives à la protection des données.
- Des réunions régulières peuvent être organisées entre le DPO et la direction générale, ou le responsable de la protection de la vie privée, ou le responsable des questions juridiques et de conformité, ou d'autres fonctions internes de l'entreprise ayant une incidence sur le risque lié à la protection de la vie privée.

Aide

- Facilite l'accès des fonctionnaires de l'Autorité aux documents et informations corrects et nécessaires
- Intervenir auprès de la direction générale et faciliter l'interprétation et l'application de la réglementation en matière de protection de la vie privée au sein de l'entreprise.

Communication en temps utile

- Les coordonnées exactes et actualisées du DPO devront être communiquées en temps utile à l'Autorité.
- Les coordonnées du DPO doivent être communiquées en interne au sein de l'entreprise et doivent figurer dans les documents relatifs à la protection de la vie privée, tels que les avis de confidentialité et les registres des activités de traitement.

LE DPO ET L'ENTREPRISE

LE DPO ET L'ENTREPRISE

- Le DPO peut être lié à l'entreprise par un contrat de travail, mais ce n'est pas obligatoire.

- Le DPO peut être un employé de l'entreprise ou un consultant externe, mais dans tous les cas, l'activité doit être exercée indépendamment des autres tâches et activités déjà réalisées pour l'entreprise.

- En outre, le PFPDT recommande que le rôle du DPO soit séparé des autres types de conseil (par exemple, conseiller en matière de protection de la vie privée, conseiller juridique) et de la représentation légale de la même entreprise (par exemple, le PDG).

COMMENT NOMMER LE DPO

Si un professionnel interne est choisi, une nomination spécifique en tant que “conseiller à la protection des données" doit être formalisée.

Si, en revanche, une personne externe est choisie, cette nomination fera partie intégrante d'un contrat de service établi.

LES ERREURS À ÉVITER

Dans le choix d'un DPO :

Considérer la nomination comme une simple formalité

Recherche d'économies maximales au détriment du service (en particulier pour les DPO externes)

Choix d'une personnalité non indépendante en situation de conflit d'intérêts

Principales solutions pratiques :

- Formaliser le temps alloué aux activités du DPO et le temps alloué aux autres tâches de bureau
- Prévoir un budget de formation pour la formation continue (pour les DPO internes)
- Garantir les installations de soutien nécessaires

AVANTAGES ET INCONVÉNIENTS

Pas d'approche unique | flexible en fonction de la réalité

	DPO interne	DPO externe
+	Connaissance approfondie de l'entreprise	Moins de problèmes d'indépendance
+	Influence (pour mettre en œuvre la protection de la vie privée dans l'entreprise)	Expérience des relations avec le PFPDT
+		Connaissance spécialisée des questions relatives à la protection de la vie privée
-	Conflits d'intérêts potentiels	Moins bonne connaissance de l'organisation/du secteur
-	Coût	Moins de présence dans l'organisation (temps disponible)
-	Trouver le bon candidat	

UNE ÉQUIPE POUR LE DPO ?

UNE ÉQUIPE POUR LE DPO

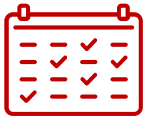
Les individus, les compétences des individus et leurs points forts peuvent être combinés afin que différents individus, travaillant en ÉQUIPE, puissent suivre les différentes activités de manière plus efficace.

Il est recommandé de **répartir clairement les tâches** au sein des équipes de DPO et d'attribuer au DPO le rôle de "personne de contact/chef d'équipe" auprès de l'entreprise. Il serait **utile de** préciser ces points dans le contrat de service.

L'ACTIVITÉ DU DPO

DOCUMENTATION DPO

Règlement relatif aux modalités de prestation du service de DPO



Plan de suivi et d'activités du DPO

Rapports et procès-verbaux

Chaque réunion du DPO doit faire l'objet d'un compte rendu spécifique indiquant les contrôles effectués, les points critiques et les conformités.

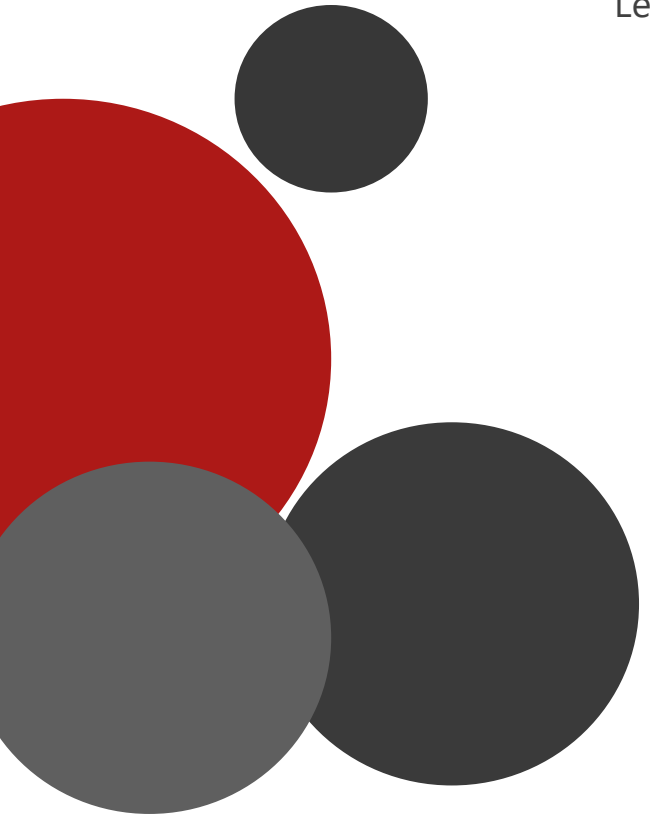
Un rapport annuel doit être présenté à la direction générale pour expliquer les résultats des réunions et des activités de suivi susmentionnées.

RÈGLEMENT SUR LES MODALITÉS DE FOURNITURE DU SERVICE DPO

Le DPO, qu'il soit interne ou externe, rédige le règlement du service, qui décrit :

- Les tâches du DPO
- La composition du DPO (seul ou en équipe)
- Les modalités de programmation de l'activité (par exemple, la fréquence des réunions, les modalités de convocation, la définition du lieu, la fourniture de procès-verbaux/rapports).
- Comment conserver et accéder aux procès-verbaux/rapports
- Comment conserver et accéder aux documents/flux
- la manière dont les vérifications/interventions sont effectuées (par exemple, citer le plan d'activités, prévoir des contrôles programmés ou à la demande de l'entreprise)

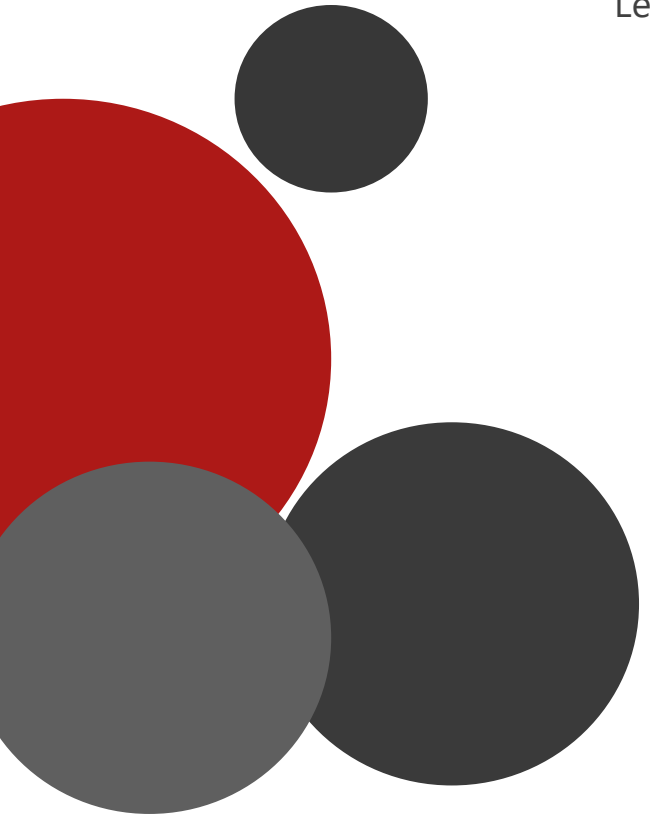
RÈGLEMENT SUR LES MODALITÉS DE FOURNITURE DU SERVICE DPO



Le DPO, qu'il soit interne ou externe, rédige le règlement du service, qui décrit :

- Les hypothèses et les modalités d'implication des parties externes
- Les ressources physiques et financières reconnues (sans préciser le montant, mais en se référant au contrat de service), en veillant à préciser les dépenses supplémentaires éventuelles pour les voyages/audits.
- Les méthodes de rapport du DPO (par exemple, courriers électroniques confidentiels, avis, procès-verbaux/rapports, convocations de la direction, rapports périodiques).
- Clause de confidentialité
- Modalités de modification du règlement

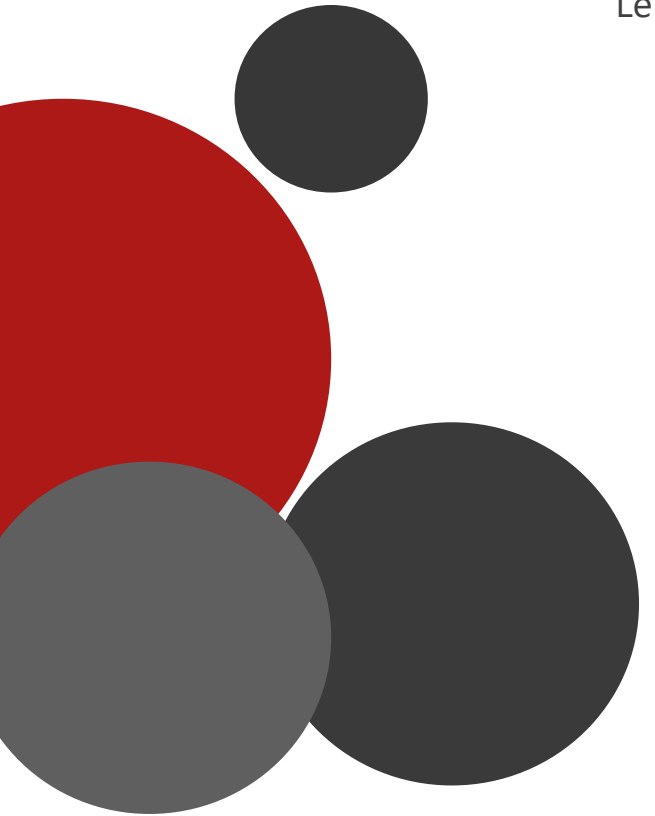
RÈGLEMENT SUR LES MODALITÉS DE FOURNITURE DU SERVICE DPO



Le DPO, qu'il soit interne ou externe, rédige le règlement du service, qui décrit :

- Les éléments de responsabilité (par exemple, la formation/information du personnel, la gouvernance d'entreprise [procurations, pouvoirs, etc.], l'adoption de mesures de sécurité technique) ;
- Gestion de la documentation du service DPO (archivage adéquat des procès-verbaux des DPO et de leurs annexes) ;
- La manière dont les entretiens sont menés avec les cadres supérieurs/représentants de zone ;
- La possibilité de donner des avis sur les AIPD et de contrôler leur bon déroulement ;

RÈGLEMENT SUR LES MODALITÉS DE FOURNITURE DU SERVICE DPO



Le DPD, qu'il soit interne ou externe, rédige le règlement du service, qui décrit :

- Flux d'informations standard vers le DPO (par exemple, cas de violation de données, demandes de la personne concernée, demandes de l'autorité, etc ;)
- Le DPO transmet périodiquement des informations à la direction (par exemple, un rapport semestriel/annuel sur les activités du DPO) ;
- Documents à vérifier (par exemple, avis de confidentialité, évaluation des risques)
- Vérification de l'établissement et de la mise à jour du registre des activités de traitement ;

LE DPO DANS LE SECTEUR PUBLIC

LE DPO DANS LE SECTEUR PUBLIC

Chaque organe fédéral désigne un DPO.
Plusieurs organes fédéraux peuvent désigner conjointement un conseiller à la protection des données.

Les mêmes obligations et spécifications que dans le secteur privé restent applicables
(par exemple, accès, indépendance et publication des coordonnées du délégué à la protection des données sur Internet et notification au PFPDT)

DPO
=
WHISTLEBLOWER?

DPO=WHISTLEBLOWER?

Est-il envisageable que le délégué à la protection des données soit tenu d'informer l'autorité si le responsable du traitement agit en violation de la législation sur la protection des données et commet une infraction pénale ?

Le DPO n'est pas le dénonciateur de privacy !

PRIVACYDESK®
SUISSE

MERCI !

Gianfranco Valsecchi

privacydesk.ch

info@privacydesk.ch