Table des matières

1. Introduction

Le paysage de la protection de la vie privée et des données évolue à un rythme effréné.

Le Délégué à la Protection des Données (ci-après « Data Protection Officer » ou « DPO ») joue un rôle important de conseiller et de superviseur en matière de conformité à la protection des données et de gestion de la vie privée dans les entreprises, afin de garantir la sauvegarde de la liberté et des droits fondamentaux des personnes concernées.

Dans cette optique, dpo pro, l'Union professionnelle des Délégués à la protection des données belge, a décidé d'élaborer un code de déontologie.

Ce code de déontologie contribue à la bonne application du règlement 2016/679 du 27 avril 2016 et des lignes directrices pour le DPO adoptées par le groupe de travail Article 29 (WP 243) le 5 avril 2016, et décrit les règles de conduite applicables aux missions du DPO.

Le code de déontologie permet de clarifier ce que les organisations peuvent attendre de la collaboration avec leur DPO et renforce la confiance mutuelle entre organisations et professionnels de la vie privée, garantissant une approche respectueuse de la confidentialité, de la qualité et de l'intégrité des conseils et des interventions du DPO. Ce code permet également aux entreprises de percevoir le niveau et le type d'assistance qu'elles doivent fournir au délégué à la protection des données afin de contribuer au succès de ses missions.

En signant ce code de déontologie, le DPO prend un engagement ferme.

OBJECTIF ET CONCEPTION

Le code de déontologie des DPO établit plusieurs principes comportementaux et éthiques essentiels pour tout DPO. Ce code est avant tout un outil d'orientation et de qualité. Le code soutient les DPO dans leur quête d'un travail professionnel et de qualité. Il peut également aider les mandataires et les employeurs des DPO à formuler leurs exigences de qualité.

PÉRIMÈTRE

Le Code de déontologie s'applique au DPO visé à l'article 37 du RGPD.

Le code de déontologie contient les principes fondamentaux de la déontologie et de l'éthique, ainsi que les règles de conduite à respecter dans l'exercice des fonctions de DPO.

2. Dispositions générales

2.1. DÉFINITIONS

dpo pro : Union professionnelle des Délégués à la protection des données belges

Code de déontologie : un code de déontologie réglemente la manière dont une profession ou une activité est exercée en vue d'adhérer à une éthique particulière. Il s'agit d'un ensemble de droits et d'obligations qui régissent une profession, la conduite de ceux qui l'exercent, les relations entre eux et leurs clients ou leur public cible.

Délégué à la Protection des Données (DPO) : Le Délégué à la Protection des Données, la personne physique responsable de la conformité au RGPD, officiellement et soit exigé par l'article 37 du RGPD, soit désigné volontairement par un responsable du traitement ou un sous-traitant. Dans le cadre due ce code de déontologie nous avons opté pour la dénomination « DPO ».

Données personnelles : Toute information relative à une personne physique identifiée ou identifiable ("personne concernée"), conformément aux dispositions de l'article 4 du RGPD.

Déontologie : la déontologie est l'ensemble des règles et des devoirs qui régissent les tâches à accomplir dans le cadre de l'exercice d'une profession.

Mandataire : la personne physique ou morale qui bénéficie des services d'un professionnel (les DPO externes). La coopération entre ces deux acteurs est déterminée par les dispositions légales applicables aux relations civiles, administratives, commerciales ou de travail.

Personne concernée : la personne identifiée ou identifiable dont les données personnelles font l'objet d'un traitement en vertu des dispositions de l'article 4 du RGPD.

Règlement Général sur la Protection des données ou RGPD : Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après " RGPD ").

Responsable du traitement : la personne physique ou morale qui détermine les finalités et les moyens du traitement conformément aux dispositions de l'article 4 du RGPD.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite les données pour le compte du responsable du traitement, conformément aux dispositions de l'article 4 du RGPD.

2.2. ADOPTION DU CODE DE DÉONTOLOGIE

Le code de déontologie, ainsi que toute modification ultérieure, est approuvé par l'assemblée des membres de dpo pro par vote. Le vote est conforme à la majorité déterminée pour l'Assemblée Générale.

Le code de déontologie est ensuite rendu public par tous les moyens possibles, y compris la publication sur le site web de l'union professionnelle dpo pro et d'autres canaux de communication que le Conseil d'Administration de dpo pro estime appropriés.

Le code entre en vigueur un mois après sa publication, également en cas de modification.

2.3. DIFFUSION - PUBLICATION

Le code de déontologie de dpo pro peut être :

- communiqué aux personnes concernées ;
- être mis à la disposition de l'ensemble de l'organisation (associations de travailleurs, employés, etc.) ;
- annexé au contrat de travail d'un DPO ;
- cité comme document de référence dans le cadre des formations d'initiation et de perfectionnement aux métiers liés à la protection des données personnelles ;
- cité dans les contrats avec les clients et les mandataires (pour un DPO externe) ;
- mentionné à des fins de recrutement dans les postes vacants de DPO ;
- être présenté par un sous-traitant à un responsable du traitement afin de démontrer qu'il fournit, entre autres moyens techniques et organisationnels appropriés, les garanties nécessaires au sens de l'article 28 du RGPD.

2.4. L'INVOCATION DU CODE DE DÉONTOLOGIE

Le présent code de déontologie peut être invoqué par tous les DPO membres de dpo pro, s'ils le souhaitent, vis-à-vis d'un responsable de traitement, d'un sous-traitant, d'un employeur, des partenaires internes et externes des organisations, de l'autorité, ainsi que vis-à-vis des personnes concernées au sens de l'article 4 du RGPD.

3. Le métier de Délégué à la Protection des Données

3.1. Définition de la profession

Dans le cadre de ce code de déontologie, nous considérons comme Délégué à la Protection des Données la personne physique ou morale responsable du respect du RGPD, formellement requis par l'article 37 du RGPD, ou volontairement désigné par un responsable du traitement ou un sous-traitant.

3.2. Tâches du DPO

Le Délégué à la Protection des Données à un rôle à la fois consultatif et de supervision. Il prodigue des conseils sur la manière de traiter les données personnelles dans le respect de la réglementation et vérifie également si ces conseils ont été traduits de manière optimale dans la pratique. En outre, il est également le lien entre l'entreprise et les autorités, qui, dans le cas de la Belgique, est l'Autorité de Protection des Données (APD).

Les missions du DPO comprennent, dans tous les cas, les tâches prévues à l'article 39 du RPGD qui sont, pour rappel :

- fournir des avis et des conseils concernant le respect de la vie privée et la protection des données tant envers le responsable de traitement que le sous-traitant ;
- contrôler le respect de la réglementation et des procédures et règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel ;
- informer et sensibiliser les employés et la direction sur le respect des règles de protection des données personnelles ;
- fournir des conseils et une interprétation dans le cadre des analyses d'impact sur la protection des données (enquête sur les effets et les risques possibles du traitement des données) ;
- coopérer et faire office de point de contact avec l'Autorité de Protection des Données (APD).

Ces tâches sont complétées par les activités suivantes :

- évaluer de façon continue et indépendante la conformité de l'entreprise avec la réglementation et les politiques internes de protection des données et de la vie privée.
  Le DPO pilote la définition et la mise en œuvre de politiques, de lignes directrices, de processus de contrôle et de règles pour la protection efficace des données à caractère personnel et pour le respect des libertés et droits fondamentaux des personnes concernées tant par le responsable du traitement que par le sous-traitant ;
- veiller à être consulté avant la mise en place de tout nouveau traitement ou de toute modification substantielle d'un traitement actif ;
- collecter et accompagner la documentation des activités de traitement des données dans le registre ;
- traiter les demandes d'exercice des droits et les plaintes des personnes concernées (membre du personnel, clients, patients, etc.) de toutes les parties prenantes ;
- prodiguer des conseils sur des mesures de sécurité et des technologies de support à la conformité au RGPD tels qu'un système de gestion électronique des documents ou un système de gestion d'archivage électronique ;
- faciliter la réalisation des audits et des contrôles ;
- préparer un rapport annuel sur ses missions, décrivant les actions entreprises au cours de l'année écoulée et soulignant les progrès accomplis et les éventuelles difficultés rencontrées ;
- informer le responsable du traitement ou le sous-traitant de son évaluation du niveau de conformité de l'organisation ;

- en cas de non-conformité, signaler au responsable du traitement ou au sous-traitant tous les éléments non conformes et les risques inhérents détectés, et proposer des mesures juridiques, organisationnelles ou techniques pour rendre l'organisation conforme et réduire ou éliminer les risques ;
- assurer ses missions en respectant la confidentialité des informations et de la documentation du responsable du traitement ou du sous-traitant, les conserver de manière sécurisée et ne pas les utiliser ou les conserver en dehors du strict cadre de sa mission.

Pour exercer correctement ses fonctions, le DPO doit :

- un accès facile et inconditionnel au responsable du traitement, au sous-traitant ou au mandataire ou au responsable direct du traitement et être en contact direct avec la direction de l'organisation ;
- s'impliquer en temps utile et de manière appropriée dans toutes les questions relatives à la protection des données ;
- recevoir du responsable du traitement ou du sous-traitant tous les moyens nécessaires et appropriés pour s'acquitter correctement de la fonction ou de la mission et être en mesure de signaler clairement et promptement tout manquement à cet égard. Cela concerne notamment :
  a) des informations et une documentation suffisantes, pertinentes et fiables pour étayer ses avis, décisions et recommandations ;
  b) un accès facilité aux interlocuteurs ayant les aptitudes et les compétences nécessaires au sein de l'entreprise ;
  c) l'assistance, la formation, les ressources et les fonds ;
  d) la décharge d'autres tâches ;
- être informé de tout projet (et de toute partie du projet) impliquant l'utilisation de données à caractère personnel afin de pouvoir examiner sa conformité et fournir des conseils à cet égard ;
- veiller à ce que ses recommandations motivées et commentées soient dûment prises en compte. Si ses recommandations ne sont pas retenues, il convient d'en fournir les raisons ;
- être en mesure de mener ou de diriger toute action par laquelle il peut juger du niveau de conformité de l'organisation, objectiver les éventuels états non conformes (gravité, impact potentiel sur les personnes concernées, origine, responsabilité, etc.). Pour mener à bien ces tâches, le DPO doit solliciter toutes les informations nécessaires au responsable du traitement, au sous-traitant ou au mandataire afin de tenir la tenue du registre des traitements ou s'assurer que celui-ci est tenure de manière conforme à l'article 30 du RGPD ;
- être consulté avant toute enquête susceptible d'avoir un impact sur les données personnelles et être mis en mesure de vérifier, voire de réaliser, sa mise en œuvre. Si nécessaire, recommander la réalisation de telles enquêtes ;
- être étroitement associé à tout ce qui concerne la communication des violations de la protection des données (préparation, enquête sur les incidents et décision de les signifier au superviseur et de les communiquer aux personnes, enquête a posteriori, réexamen des mesures prises pour protéger les données, etc.) ;
- être facilement et directement accessible, que ce soit au sein de l'organisation où il exerce ses fonctions ou depuis l'environnement extérieur. À cette fin, les coordonnées (adresse postale, numéro de téléphone, adresse électronique) du DPO seront communiquées par tous les moyens réalisables.
  Si le DPO travaille pour un groupe de sociétés et/ou d'organisations, il doit être facilement accessible depuis chaque organisation, que ce soit par les personnes concernées ou par les

autorités de contrôle, mais aussi par chaque organisation dont il est le DPO. Il veille donc à ce que ses coordonnées soient diffusées de manière appropriée ;

3.3 COMPÉTENCES, CONNAISSANCES, SAVOIR-FAIRE, ATTITUDE

Le DPO met en œuvre les connaissances, les compétences et l'expérience nécessaires à l'accomplissement de sa mission.

Le RGPD stipule que le DPO dispose des qualifications requises pour remplir ses missions. Si le DPO est une personne morale, l'exigence de qualification doit être remplie par la personne désignée par la personne morale pour accomplir les missions.

Le DPO doit maintenir ses compétences et ses connaissances dans les domaines respectifs et s'efforcer de les améliorer et de les enrichir en permanence en suivant les évolutions juridiques, technologiques et sociales - si nécessaire par une formation continue appropriée.

4. Principes éthiques

Le code identifie 5 principes de professionnalisme pour le DPO. Sur base de ces principes, chaque DPO est censé se comporter de manière professionnelle et s'engager à fournir des prestations de qualité. En d'autres termes, le DPO agit de manière :

- Honnête et crédible
- Intègre
- Indépendant, objectif et impartial
- Confidentielle
- Loyale et collégiale

Ces normes sont exprimées de manière concise ci-dessous par plusieurs déclarations :

HONNÊTETÉ ET CRÉDIBILITÉ

L'honnêteté et la crédibilité d'une personne constituent la mesure de la fiabilité au sein de toute organisation.

Chaque DPO traite, dans l'exercice de ses fonctions et en toutes circonstances, les informations qu'il fournit avec soin et veille à ce que ces informations soient vérifiables et indiscutables.

Ainsi, le DPO démontre qu'il dispose des compétences appropriées pour exercer ses missions. Ce comportement malhonnête pourrait compromettre la crédibilité du DPO et être préjudiciable à la sécurité et à la conformité des traitements de données pour lesquelles le responsable du traitement lui demande conseil et support.

INTÉGRITÉ

Chaque DPO doit toujours s'acquitter de sa fonction et des tâches qui lui sont confiées au mieux de ses capacités, avec intégrité professionnelle et efficacité. Chaque DPO se doit d'être conscient de l'importance de ses tâches et de sa fonction, et respecter les normes élevées de l'éthique professionnelle dans ses actions.

Dès lors, le DPO agira toujours dans le respect des principes imposés par la réglementation, par les règles internes à l'entreprise et par le présent code de déontologie, sans se laisser corrompre par des demandes inappropriées visant à servir des intérêts individuels, telles que passer sous silence des traitements de données inacceptables et non conformes, à la demande du responsable de traitement ou du sous-traitant. En cas de conflit entre les règles internes de l'entreprise et le code de déontologie, le DPO entamera un dialogue avec la direction.

INDÉPENDANCE, OBJECTIVITÉ ET IMPARTIALITÉ

Le DPO évalue les informations et la documentation reçues de manière équilibrée et porte son jugement sans être influencés en cela par ses propres intérêts ou ceux de tiers.

Le DPO doit faire preuve d'indépendance, d'objectivité et d'impartialité dans l'exercice de ses fonctions.

Chaque DPO est tenu d'éviter toute situation qui pourrait donner lieu ou sembler donner lieu à un conflit d'intérêts. Il y a conflit d'intérêts lorsque le DPO a des intérêts privés ou personnels qui pourraient ou semblent influencer l'exercice impartial et objectif de ses fonctions, ou lorsqu'il y a contradiction entre les intérêts de (la direction de) l'entreprise dans laquelle il occupe le poste de DPO et les siens.

L'employeur ou le client doit s'assurer que le DPO peut travailler en toute indépendance et communiquer directement et indépendamment avec le plus haut niveau de direction.

En tant que DPO, il n'a pas à répondre à un supérieur hiérarchique. Dans le cadre de sa fonction, il dispose de toute la liberté d'organisation et de décision.

CONFIDENTIALITÉ

Chaque DPO respecte la valeur et la propriété des informations qu'il reçoit et ne divulgue pas d'informations sans autorisation appropriée, sauf s'il existe une raison légale ou professionnelle de le faire. Il est soumis au secret professionnel et se doit de respecter la stricte confidentialité des informations qui lui sont confiées ou dont il a connaissance.

LOYAUTÉ ET COLLÉGIALITÉ

Tout en devant remplir fidèlement ses obligations, le DPO doit également agir "de bonne foi".

Union professionnelle des Délégués à la Protection des Données de Belgique

Rue des Sols 8 - 1000 Bruxelles

info@dpopro.be

www.dpopro.be