OG SBC
OG Security Business Consulting

Devenez Data Protection Officer - Aperçu essentiel

27 Février 2025

NOS INTERVENANTS

JAMAL SAAD

Directeur des opérations Cyber sécurité et intelligence économique chez OGSBC

CHAIMAE HAROUCHE

Consultante Cyber Sécurité

LAMYAE BAKKARI

Modératrice
Assistante Administrative et Commerciale

Plan de la présentation

Qui sommes-nous ?

OGSBC est un cabinet de Conseil, d'Audit en cyber sécurité, délivre des services de gestion des infrastructures et de sécurité de l'information.

Délivre des services de Protection des Entreprises et d'Intelligence Economique.

Délivre des formations en Cyber sécurité auprès des professionnels de SI.

Ce que nous vous offrons

CENTRE DE FORMATION AGRÉE

Des formations de très haut niveau avec des certifications délivrées par des organismes reconnus.

AUDIT ET CERTIFICATION

Audit de vos systèmes existants pour identifier les failles de sécurité et obtenir des certifications de sécurité.

CONSEIL ET ANALYSE DES RISQUES CYBER

Un accompagnement personnalisé pour vous aider à évaluer et à gérer vos risques cyber.

Protection des Entreprises & Intelligence Economique

Des solutions sur mesure pour protéger vos données sensibles et votre réputation.

OG SBC
OG Security Business Consulting

CENTRE DE FORMATION AGRÉE

Nous offrons plusieurs formations en collaboration avec des organismes internationaux.

PECB

EC-Council

Nos formations certifiantes de PECB

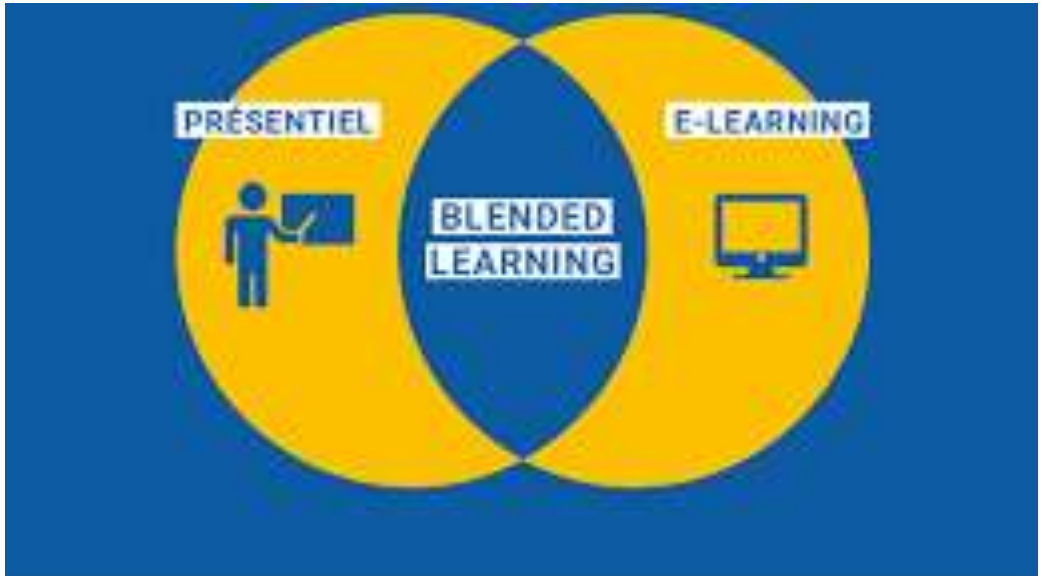
- ISO/CEI 27005 Risk Manager
- EBIOS Risk Manager
- ISO/IEC 27001 Lead Implementer
- ISO/CEI 27001 Lead Auditor
- Certified Data Protection Officer
- ISO/IEC 27701 Lead Implementer
- ISO/IEC 27035 Lead Incident Manager
- Lead Cloud Security Manager
- Lead Cybersecurity Manager

Nos formations certifiantes EC-COUNCIL

- Certified Chief Information Security Officer
- Certified Ethical Hacker
- EC-Council Certified DevSecOps Engineer
- Certified Cloud Security Engineer
- Certified Network Defender
- Certified Cloud Security Engineer
- Certified Penetration Testing Professional
- Certified Blockchain Professional
- Certified Threat Intelligence Analyst
- Certified SOC Analyst
- Certified Cybersecurity Technician
- Web Application Hacking and Security

Mode de formations

- **EN PRÉSENTIEL**
- **SELF-STUDY**
- **HYBRIDE**



TÉLÉCHARGER NOTRE CATALOGUE DE FORMATIONS [ICI]

OG SBC
OG Security Business Consulting

Nos formations en ligne

udemy

OSIR
CYBER SECURITY INSTITUT

OSIR
CYBER EDUCATION

Nous ont fait Confiance

LE DPO

- La notion de DPO n’est pas nouvelle même si la directive 95/46/CE n’apportait pas de contrainte à la désignation

- En France, le CNIL recommandait la nomination d’un CIL

LE DPO

- Le DPO est un élément important dans le processus d'accountability (responsabilité).

- Il facilite le respect des règles et sa présence peut-être un avantage « marketing » auprès des clients.

LE DPO

- La responsabilité du DPO

Le respect de la protection des données relève de la responsabilité du sous-traitant ou du responsable du traitement.

Le délégué à la protection des données n'est donc pas responsable en cas de non-respect du règlement (sauf si le DPO enfreint intentionnellement les dispositions pénales de la loi)

Désignation d'un DPO

Cas où la désignation est obligatoire

Article 37 paragraphe 1

- Lorsque le traitement est effectué par « **une autorité ou un organisme public** »; (sauf « *les juridictions agissant dans l'exercice de leur fonction juridictionnelle* » – Directive (UE) 2016/680 article 32)

(Il est recommandé aux organismes privés chargés d'effectuer des missions de service public ou exerçant l'autorité publique de désigner un DPO)

- Lorsque les **activités de base** du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à **grande échelle** des personnes concernées;

- Lorsque les **activités de base** du responsable du traitement ou du sous-traitant consistent en un traitement à **grande échelle** de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Désignation d'un DPO

« une autorité ou un organisme public »

- Dans le RGPD, il n'y a pas de définition expliquant ce qu'est « **une autorité ou un organisme public** »

Mais le G29 considère que c'est le droit national qui doit apporter une définition.

ARTICLE 29
Data Protection Working Party

« **une autorité ou un organisme public** »

inclut donc les autorités nationales, régionales et locales et en fonction du droit national, d'autres organisations de droit public

Désignation d'un DPO

Les «activités de base»

Article 37 paragraphe 1 points b et c

- Le RGPD désigne les **« activités de base du responsable du traitement ou du sous-traitant »**

Le considérant 97 en précise le sens:

« activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaires »

Les « **activités de base** » sont les opérations essentielles pour atteindre l'objectif du responsable du traitement mais cela n'exclut pas le traitement faisant partie intégrante de l'activité du RT

Désignation d’un DPO

Le suivi à «grande échelle»

Article 37 paragraphe 1 points b et c

- L’article 37 paragraphe 1 points b et c impose la nomination d’un DPO lorsqu’un traitement est réalisé à grande échelle mais ne définit pas le terme « **grande échelle** » et ne donne pas de chiffre

- Le considérant 91 apporte quand même des précisions en indiquant que cela concerne les « **Volumes considérables de données au niveau régional, national ou supranational** »

Désignation d'un DPO

Le suivi à «grande échelle»

Article 37 paragraphe 1 points b et c

- Afin de définir si un traitement est réalisé à « grande échelle », le G29 recommande que les éléments suivants soient pris en compte

  - le nombre de personnes concernées, en valeur absolue ou par rapport à la population concernée;
  - le volume de données et/ou le spectre de données traitées;
  - la durée des activités de traitement;
  - l'étendue géographique de l'activité de traitement.

ARTICLE 29
Data Protection Working Party

Désignation d'un DPO

Le suivi à «grande échelle»

Article 37 paragraphe 1 points b et c

- Exemples de traitement à grande échelle:

Traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités;

Traitement des données de voyage des passagers utilisant un moyen de transport public urbain (suivi par titre de transport …);

Traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités;

Désignation d’un DPO

Le suivi à «grande échelle»

Article 37 paragraphe 1 points b et c

- Exemples ne constituant pas un traitement à grande échelle:

Traitement, par un médecin, ou un autre professionnel de santé, exerçant à titre individuel, des données de ses patients;

Traitement des données à caractères personnel liés aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

Désignation d’un DPO

Désignation sans obligation

Article 37 paragraphe 1

- Lorsque la nomination d’un DPO n’est pas nécessaire, il convient au responsable de traitement de documenter l’analyse effectuée pour arriver à cette conclusion. Analyse à présenter en cas de contrôle.

L’analyse doit être faite à nouveau en cas de nouveau traitement ou de modification qui entrerai dans le champs de l’article 37 paragraphe 1.

Désignation d’un DPO

Désignation volontaire

Article 37 paragraphe 1

- Lorsque l’organisme désigne volontairement un DPO hors cadre obligatoire de l’article 37 paragraphe 1, alors les articles 37 à 39 (désignation, fonctions, missions) s’appliquent comme si la désignation avait été obligatoire.

- Sinon lorsque **l’organisme ne souhaite pas désigner un DPO** lorsqu’elle n’en a pas obligation, elle peut utiliser une personne qui sera chargée de la protection des données à caractère personnel mais **cette personne ne peut avoir le titre de DPO**. Il ne doit pas y avoir ambigüité quand à la fonction, les missions et le statut

Désignation d'un DPO

Le DPO du sous-traitant

Article 37

- Le responsable comme le sous-traitant sont concernés par la désignation d'un DPO.
- Lorsque les 2 ont obligations de désigner un DPO, chacun a le sien et les 2 DPO doivent collaborer
- Il peut arriver que le responsable de traitement doivent désigner un DPO alors que son sous-traitant n'a pas cette obligation.

 (Le Sous-traitant peut en nommé un afin de suivre un code de bonne pratique en matière de sécurité des données personnelles)

Désignation d'un DPO

Un seul DPO pour un groupe d'entreprises

Article 37 paragraphe 2

Un groupe d'entreprises est autorisé par l'article 37 paragraphe 2, à désigner un seul DPO à la condition qu'il soit ***«facilement joignable à partir de chaque lieu d'établissement»,*** et remplit ses missions:

- **Point de contact pour les personnes concernées**

  Article 38, paragraphe 4: «*Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement*».

- **Point de contact pour l'autorité de contrôle**

  article 39 paragraphe 1 point e: «*faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet*».

- **Informe et conseille l'organisation**

  article 39 paragraphe1 point a: «*informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement*»

Désignation d'un DPO

Notion de joignabilité et localisation du DPO

Article 37 paragraphe 2

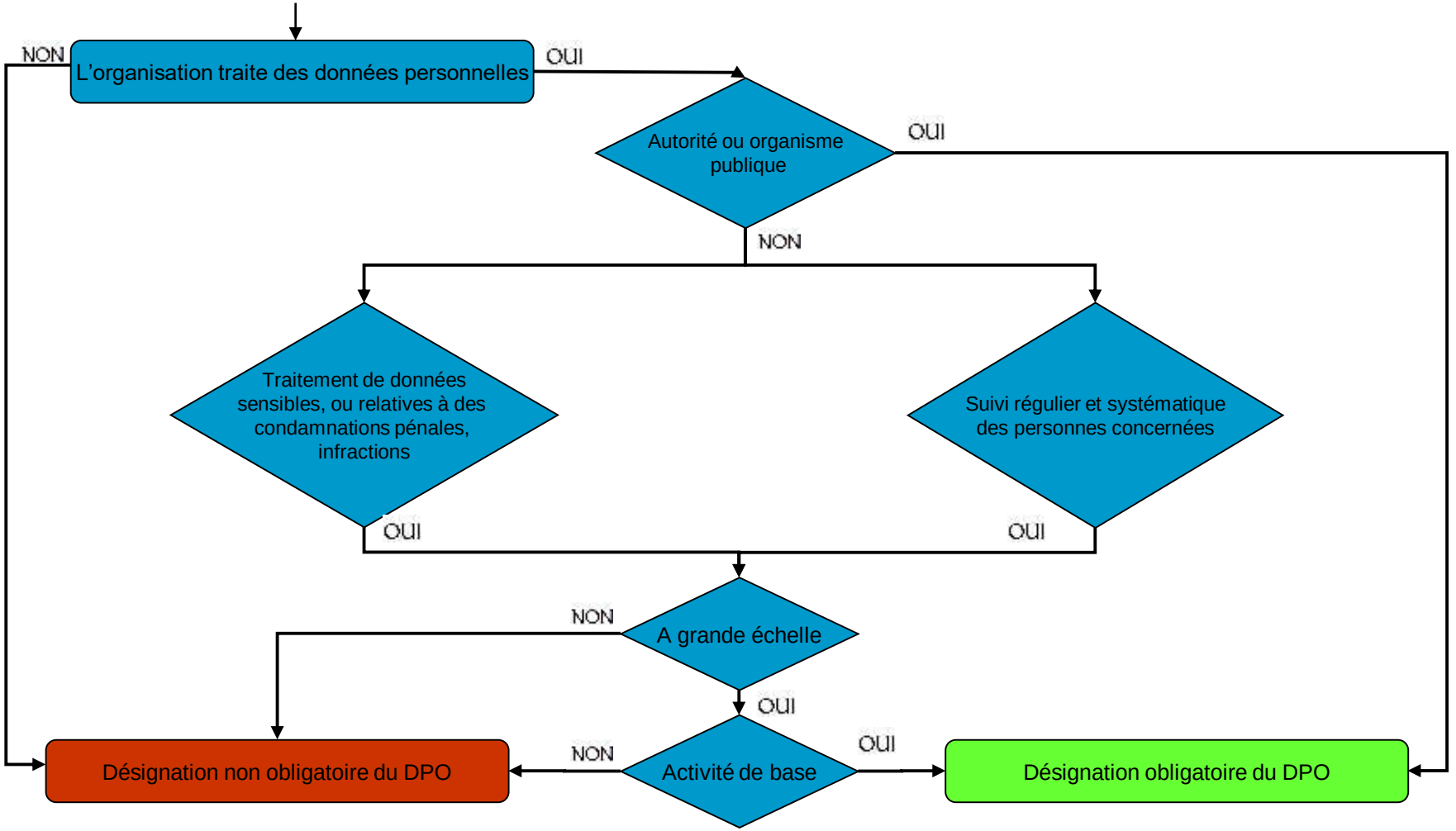
En respect de l'article 37 paragraphe 2, le DPO doit être

«facilement joignable»

Afin de se conformer à cette obligation, il est conseillé d'avoir le DPO localisé dans l'Union Européenne même si le RT ou le ST n'y sont pas.

Cependant, dans les cas où, l'organisme ne possède pas d'établissement dans l'Union Européenne, le DPO peut se trouver en dehors de l'UE si son action est plus efficace.

Désignation d'un DPO



Les Fonctions du DPO

Associé a la protection des données

Article 38

- **L'article 38** indique que le **DPO** doit être « **associé**, d'une manière appropriée et en temps utile, à **toutes les questions** relatives à la **protection des données** à caractère personnel »

- L'entreprise ou l'organisme responsable de traitement et le sous-traitant doivent s'assurer que le DPO:

  - est présent lors de réunions où des décisions importantes sur la protection des données sont prises et en règle générale lors de réunion de direction.
  - a accès aux informations utiles afin de donner son avis le cas échéant.(au cas où l'avis du DPO n'a pas été suivi, le groupe G29 recommande de documenter les raisons).
  - est informé de tout incident de sécurité (perte, violation …)

Les Fonctions du DPO

Les ressources octroyées au DPO

Article 38 paragraphe 2

- **L'article 38** paragraphe 2 impose que l'organisme fournisse les ressources nécessaires au DPO afin d'exercer ses fonctions et ses missions de façon optimum. Pour cela, le DPO doit avoir:

- Le soutien actif de la direction.
- Le soutien actif (supports, informations) de l'ensemble des services (RH, juridique, informatique etc…)
- Suffisamment de temps pour accomplir chaque tâche.
- Les ressources financières et matériels
- Être connu (missions et fonctions) de l'ensemble des salariés suite à une communication officielle interne
- Formation continue afin de maintenir à niveau ses compétences
- Constituer une équipe, sous sa responsabilité, lorsque la taille de l'organisme le nécessite.

Les Fonctions du DPO

Indépendance

Article 38 paragraphe 3

Le délégué doit agir d'une manière indépendante et bénéficier d'une protection dans l'exercice de ses fonctions.

Le DPO ne peut pas être

- tenu d'adopter un point de vue concernant un avis.
- empêché de consulter l'autorité de contrôle ou d'enquêter sur une plainte

Mais ses actions doivent rester dans le cadre de ses missions définies dans l'article 39

Les Fonctions du DPO

Indépendance

Article 38 paragraphe 3

Si le responsable de traitement ou le sous-traitant prend des décisions contraires au respect du RGPD et cela contre l'avis du DPO

le DPO a le pouvoir d'informer au niveau le plus élevé de l'organisme son avis divergent.

Les Fonctions du DPO

Licenciement ou sanction

Article 38 paragraphe 3

L'indépendance et l'autonomie du DPO sont renforcées par l'article 38 paragraphe 3 qui indique que le DPO ne peut pas être « ***relevé de ses fonctions ou pénalisé par le responsable de traitement ou le sous-traitant pour l'exercice de ses missions*** »

(il ne peut pas être relevé de ses fonctions si, par exemple, il conseille une étude d'impact sur un traitement à risque alors que le responsable de traitement pense le contraire)

Mais il peut être licencié pour des motifs autres que l'exercice de ses fonctions de délégué (en cas de vol, fautes graves …)

LE DPO
Conflits d’intérêts

Article 38 paragraphe 6

- Les conflits d’intérêts

  Le DPO doit éviter d’être « **juge et partie** »

Il ne peut avoir de fonctions ou de rôles qui déterminent la finalités et les moyens du traitement

LE DPO
Conflits d'intérêts

Article 38 paragraphe 6

- Le RGPD permet au DPO d' « **exécuter d'autres missions et tâches » mais l'organisation doit s'assurer que « ces missions et tâches n'entrainent pas de conflit d'intérêts** »

Le **DPO ne peut exercer de rôle** qui le place dans **la position** de **déterminer les finalités et les moyens du traitement** de DCP

LE DPO
Conflis d'intérêts

Article 38 paragraphe 6

- Le G29 recommande aux responsables du traitement ou aux sous-traitants:
  - de recenser les fonctions qui seraient incompatibles avec celle du DPO;
  - d'établir des règles internes pour éviter les conflits d'intérêts et d'inclure une explication plus générale des conflits d'intérêts;
  - de déclarer que leur DPO n'a pas de conflit d'intérêt en relation avec sa fonction de DPO (afin de mieux faire connaître cette exigence);
  - de prévoir des garanties dans le règlement intérieur de l'organisation pour éviter ces conflits;

Les Mission du DPO

Contrôle du Respect du RGPD

Article 39 paragraphe 1 point b

- Le DPO a pour mission de contrôler le respect du RGPD en:
  - Recueillant les informations permettant de recenser les activités de traitement
  - Analysant et vérifiant la conformité des activités de traitement
  - Informant et conseillant le responsable du traitement ou le sous-traitant et en formulant des recommandations

    (le considérant 97 indique aussi que le DPO « devrait aider le responsable du traitement ou le sous-traitant à vérifier le respect …du règlement »)

Les Mission du DPO

Contrôle du Respect du RGPD

Article 39 paragraphe 1 point b

- La responsabilité du DPO

Le respect de la protection des données relève de la responsabilité du sous-traitant ou du responsable du traitement.

Le délégué à la protection des données n'est donc pas responsable en cas de non-respect du règlement (sauf si le DPO enfreint intentionnellement les dispositions pénales de la loi)

L'article 24 paragraphe 1 indique que c'est le RT qui est tenu de : «**mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement** »

Les Mission du DPO

Veiller à la bonne réalisation des études d'impact

Article 39 paragraphe 1 point c

- Le DPO, comme l'indique l'article 39 para.1 C, a pour mission de « **dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35** »

L'article 35 qui indique que c'est le RT qui est en charge de réaliser, si nécessaire l'étude d'impact, et qu'il est exigé que le RT demande conseil au DPO

Les Mission du DPO

Veiller à la bonne réalisation des études d'impact

Article 39 paragraphe 1 point c

- Le G29 recommande que le responsable de traitement consulte le DPO sur les questions suivantes:

Convient-il ou non de réaliser une étude d'impact relative à la protection des données ?

Quelle est la méthodologie à suivre lors de la réalisation d'une étude d'impact ?

Les Mission du DPO

Veiller à la bonne réalisation des études d'impact

Article 39 paragraphe 1 point c

- Si le responsable de traitement n'est pas d'accord avec l'avis donné par le DPO, il doit documenter et justifier la raison de la non prise en compte de l'avis du DPO.

  L'article 24 paragraphe 1 stipule que

  « compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et **être en mesure de démontrer** que le traitement est effectué conformément au présent règlement. »

Les Missions du DPO

Informer et conseiller

Article 39 paragraphe 1 point A

- Le DPO doit informer et conseiller le responsable du traitement (ou le sous-traitant) et les autres employés qui procèdent au traitement, des obligations qu'ils ont vis-à-vis du RGPD ou d'autres dispositions du droit de l'état membres

Les Missions du DPO:

Coopérer et être le point de contact avec l'autorité de contrôle

Article 39 paragraphe 1 point D et E

- Le DPO est le point de contact de l'autorité de contrôle au sein de l'organisation. Il facilite l'accès de l'autorité aux documents et informations dans le cadre de l'exécution des missions de l'autorité comme indiqué dans les **article 57** et de ses pouvoirs: **article 58**

- **L'article 38** paragraphe 5 mentionne que le DPO est soumis au secret professionnel mais il peut demander un avis à l'autorité de contrôle comme le prévoit **l'article 39 paragraphe 1 point E**

Les Missions du DPO

Approche fondée sur les Risques

Article 39 paragraphe 2

- Le DPO doit établir des priorités en fonction du niveau de risque.
  ⇨ Prioriser les actions

Identifier les actions à mener en fonction du risque

Les Missions du DPO

Approche fondée sur les Risques

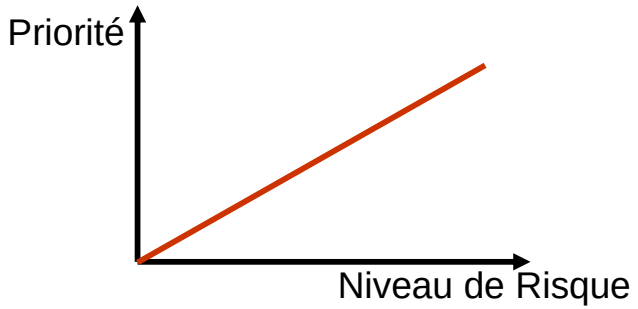
Article 39 paragraphe 2

- Le DPO doit établir des priorités en fonction du niveau de risque.

  ⇒ Prioriser les actions

Identifier les actions à mener en fonction du risque

- Mesures de sécurité en place
- Formation du personnel
- Légitimité des collectes
- Mentions d'information
- Obligations sous-traitants
- Exercice des droits des personnes



Les Missions du DPO

La tenue du registre de traitement

Article 39 paragraphe 2

- Le registre de traitement des données doit être tenu par le responsable de traitement ou le sous-traitant.

  Article 30 paragraphe 1 et 2: « *un registre des activités de traitement effectuées sous [sa] responsabilité*» ou «*un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement*».

- Cependant, l'article 39 paragraphe 1 liste les missions que le DPO doit au minimum se voir confier. Il est donc possible que le RT confie la mission de tenir le registre des traitements au DPO sous sa responsabilité (ou celle du sous-traitant le cas échéant).

Le registre des traitements est alors considéré par le DPO comme étant un outil permettant de remplir son rôle de conseil et d'information auprès du RT ainsi que de contrôle du respect du RGPD.

Niveau d’expertise du DPO

Article 37 paragraphe 5

- Le RGPD insiste sur le fait que le DPO «est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l’article 39. »

Le niveau d’expertise n’est pas précisément défini mais il doit être en corrélation avec la fonction et la complexité des opérations de traitement de données, le volume de données et la protection demandée pour les DCP. (considérant 97)

Niveau d’expertise du DPO

Article 37 paragraphe 5

- Le DPO doit avoir une très bonne connaissance :


des législations nationales et européennes relatives à la protection des données;


du **R**ègle**G**ément sur la **P**rotection des **D**onnées;


du secteur d’activité de l’organisme;


des opérations de traitement effectuées;


des systèmes d’information;


des procédures administratives, pour les entités publiques

Le DPO doit aussi être **intègre** et avoir un haut niveau de **déontologie**

OG SBC
OG Security Business Consulting

QUIZ TIME

Let's put your knowledge to the test!

Cliquez ici pour participer au Quiz

Start Now


OG SBC
OG Security Business Consulting
Question
next

Contact Us

OGSBC
OG Security Business Consulting

Call us

+212.7.08.08.08.82

+212.7.08.07.08.87

Email

contact@ogsbc.ma

Site Web

www.ogsbc.ma

OG SBC
OG Security Business Consulting

Suivez-nous sur nos réseaux sociaux

Linkedin

Instagram

Facebook