Délibération n° 2023-001 APDP/Pt/SA du 31 mars 2023
portant adoption du Référentiel général pour la formation à la protection des données personnelles au Bénin

Vu la loi n° 90-32 du 11 décembre 1990 portant Constitution de la République du Bénin, modifiée par la loi n° 2019-40 du 07 novembre 2019 ;

Vu la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, modifiée par la loi n° 2020-35 du 06 janvier 2021 ;

Vu le décret n° 2021-092 du 10 mars 2021 portant nomination des membres de l'Autorité de Protection des Données à caractère Personnel ;

Vu le décret n° 2016-513 du 24 août 2016 portant nomination de madame Félicité AHOUANDOGBO née TALON en qualité de Commissaire du Gouvernement près l'APDP précédemment, Commission Nationale de l'Informatique et des Libertés ;

Vu le règlement intérieur de l'Autorité de Protection des Données à caractère Personnel du 25 janvier 2019 ;

Vu le procès-verbal du 25 mai 2021 relatif à l'élection du bureau de l'Autorité de Protection des Données à caractère Personnel ;

Vu la délibération du 27 avril 2022 sur l'institution de la labellisation des formations en matière de protection des données personnelles au Bénin ;

Vu le procès-verbal de la session plénière du 31 mars 2023 portant adoption du Référentiel général pour la formation en matière de données personnelles

DECIDE

Article 1er :
Il est adopté un Référentiel général pour la formation en matière de données personnelles au Bénin, figurant en annexe de la présente délibération.

Article 2 :
Le Référentiel est susceptible de modification à l'initiative de l'APDP.

Article 3 :
La présente décision prend effet à compter de sa date de signature. Elle sera publiée au Journal officiel et partout où besoin sera.

Fait à Cotonou, le 29 avril 2023

Le Président

République du Bénin
Le Président
Autorité de Protection des Données Personnelles

Yvon DETCHENOU

Annexe : Référentiel général pour la formation

REPUBLIQUE DU BENIN

_____

AUTORITE DE PROTECTION DES DONNÉES PERSONNELLES

RÉFÉRENTIEL GÉNÉRAL POUR LA FORMATION A LA PROTECTION DES DONNEES PERSONNELLES

SOMMAIRE

RECOMMANDATIONS GENERALES

Ce référentiel peut être utilisé par les formateurs et organismes de formation labellisés pour garantir la qualité et la pertinence de leurs formations aux conditions suivantes.

1. Objectifs et contenu de la formation : La formation doit avoir pour objectif de transmettre les connaissances essentielles sur la protection des données personnelles, en mettant l'accent sur les aspects pratiques et les cas concrets. Le contenu de la formation doit couvrir les points essentiels du thème qui sont énoncés.

2. Qualifications et compétences des formateurs : Les formateurs doivent avoir une expérience professionnelle significative dans le domaine de la protection des données personnelles, ainsi qu'une expertise technique et pédagogique avérée. Ils doivent avoir suivi une formation spécifique sur la protection des données personnelles et être en mesure de transmettre les connaissances de manière claire et accessible. A cette fin, les formateurs et organismes de formation doivent être titulaire du label APDP Approuvé.

3. Méthodologie pédagogique : La formation doit être adaptée aux besoins des participants. La méthodologie pédagogique utilisée doit être efficace, en favorisant les interactions et les échanges d'expérience entre les participants. Pour chaque formation des supports de formation clairs et pertinents doivent être fournis aux participants.

4. Évaluation de la formation : Toute formation doit faire l'objet d'une évaluation régulière par les participants, qui doivent être invités à remplir un questionnaire d'évaluation à la fin de la formation. Les participants adressent une copie du formulaire à l'Autorité de Protection des Données Personnelles. Un modèle est disponible sur le site de l'APDP. L'organisme de formation doit également réaliser une évaluation de la prestation du formateur. Enfin le formateur doit proposer une évaluation des acquis. À défaut de cette évaluation des acquis, il ne peut être délivré qu'une preuve de participation. Une copie de chaque attestation de participation délivrée est adressée à l'APDP. Toute certification professionnelle, par évaluation, par projet, ou par validation des acquis de l'expérience (VAE) doit répondre aux modalités adoptées par l'Autorité.

5. Respect de la réglementation en vigueur : L'organisme de formation et les formateurs doivent respecter la réglementation en vigueur en matière de protection des données personnelles, notamment la loi n°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin.

6. Suivi et mise à jour des connaissances : Les formateurs et organismes de formation sont tenus de suivre régulièrement des formations pour actualiser

leurs connaissances et leur expertise en matière de protection des données personnelles. Ils doivent se conformer au cadre d’obligation de la labellisation.

Confidentialité et sécurité des données : L'organisme de formation et les formateurs doivent garantir la confidentialité et la sécurité des données personnelles des participants à la formation, en conformité avec la réglementation en vigueur.

LES THEMES

1. NOTION ET REALITES DES DONNEES PERSONNELLES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- définition légale des données personnelles au Bénin, précisions conceptuelles ;
- raisons motivant la protection des données ;
- classification des données et régime légal ;
- catégorisation pratique des données personnelles.

b. Objectifs à atteindre

La formation permet de connaître :

- et de catégoriser les données à caractère personnel suivant la nature, la sensibilité ou le niveau de criticité ;
- et d'identifier le régime juridique des données.

La formation permet de connaitre et de comprendre :

- les notions d'empreinte numérique et ses implications sur la vie privée ;
- les enjeux de la protection des données personnelles ;
- problématique du concept de la gouvernance des données personnelles en général ; problématique du concept Économies des données personnelles en général ;
- l'enjeu de souveraineté numérique.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 4 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- questions à choix multiples et questions ouvertes sur la compréhension des notions de données personnelles, de traitement de données, de responsabilité, de consentement, de finalité, de sécurité, la connaissance du cadre réglementaire en vigueur, sur les enjeux éthiques liés à la collecte et au traitement des données personnelles, notamment en termes de respect de la vie privée, de la liberté individuelle et de la dignité humaine ;

- cas pratiques qui mettent en évidence les situations où la protection des données personnelles est en jeu, afin d'évaluer la capacité des apprenants à appliquer les notions théoriques à des situations concrètes et à proposer des solutions pratiques pour garantir la protection des données personnelles, en tenant compte des exigences légales et des spécificités de chaque situation.

2. HISTOIRE ET SOURCES JURIDIQUES DE LA PROTECTION DES DONNEES PERSONNELLES AU BENIN

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- sources internationales et régionales ;
- contexte de l'institutionnalisation d'un régime de Protection des données personnelles au Bénin ;
- cadre de la protection des données personnelles au Bénin : historique, sources juridiques champ d'application (matériel et territorial) organisation de la protection, régulateur institué, protection judiciaire.

b. Objectifs à atteindre

La formation permet de connaître et de comprendre les notions de :

- données à caractère personnel ;
- le champ d'application matériel et territorial du régime de protection des Données personnelles applicable au Bénin ;
- l'articulation entre les textes relatifs à la protection des données et les autres sources de droit.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 5 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- QCM (questionnaire à choix multiples) : il est possible de poser des questions à choix multiples portant sur l'histoire et les sources juridiques de la protection des données personnelles au Bénin, avec plusieurs réponses possibles pour chaque question. Cela permet de vérifier la connaissance des apprenants sur les principaux instruments juridiques internationaux, les organes de régulation et les enjeux liés à la protection des données personnelles ;
- étude de cas : les apprenants peuvent être soumis à une étude de cas basée sur des situations réelles dans lesquelles des données personnelles sont collectées, traitées ou utilisées de manière illégale. Les apprenants doivent ensuite identifier les principaux instruments juridiques internationaux qui peuvent être utilisés pour protéger ces données personnelles, ainsi que les mesures que les entreprises peuvent prendre pour se conformer à la réglementation en matière de protection des données personnelles.
- questions ouvertes : les apprenants peuvent être invités à répondre à des questions ouvertes portant sur l'histoire et les sources juridiques de la protection des données personnelles au Bénin. Ces questions peuvent porter sur les principaux instruments juridiques internationaux, les organes de régulation, les enjeux liés à la protection des

données personnelles, les mesures que les entreprises peuvent prendre pour se conformer à la réglementation, etc.

- examen écrit: les apprenants peuvent être soumis à un examen écrit portant sur l'histoire et les sources juridiques de la protection des données personnelles au Bénin, avec des questions portant sur les principaux instruments juridiques internationaux, les organes de régulation, les enjeux liés à la protection des données personnelles, les mesures que les entreprises peuvent prendre pour se conformer à la réglementation, etc.

3. GRANDS PRINCIPES DE LA PROTECTION DES DONNEES PERSONNELLES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- Notion de principe et mise en relation avec les droits des personnes concernées et les obligations des responsables de traitements, sous-traitants et destinataire des données ;
- Les principes fondamentaux de la protection des données personnelles au Bénin :

  - ✓ le principe de la licéité ;
  - ✓ le principe de la loyauté ;
  - ✓ le principe de la transparence ;
  - ✓ le principe de la limitation de la finalité ;
  - ✓ le principe de la minimisation des données ;
  - ✓ le principe de l'exactitude des données ;
  - ✓ le principe de la limitation de la durée de conservation des données ;
  - ✓ le principe de la responsabilité ;
  - ✓ le principe de la sécurité des données.

b. Objectifs à atteindre

La formation permet de connaître et de comprendre :

- les conditions de licéité d'un traitement ;
- les conditions applicables au consentement ;
- le principe de proportionnalité et de pertinence des données ;
- les conditions applicables aux traitements portant sur des catégories particulières de données ;
- le principe de durée de conservation des données ;
- les principes de sécurité et de confidentialité des données et permet de qualifier un incident de sécurité en violation de données à caractère personnel ;
- le principe de transparence des informations et des communications avec les personnes concernées par un traitement ;
- le principe d'exactitude des données ;
- les droits dont disposent les personnes concernées ainsi que leurs modalités d'exercice.

La formation permet de connaître et de lier les principes avec les droits des personnes concernées et les obligations des responsables de traitements, sous-traitants et destinataire des données.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 6 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- QCM (questionnaire à choix multiples) : un QCM peut être utilisé pour vérifier les connaissances sur les grands principes de la protection des données personnelles tels que la collecte, le traitement, la conservation, la sécurité, la confidentialité et la finalité des données personnelles. Le QCM peut inclure des questions sur les définitions, les obligations juridiques, les mesures de sécurité et les sanctions en cas de non-conformité ;
- scénarios de vie privée : les apprenants peuvent être soumis à des scénarios de vie privée où ils doivent identifier les données personnelles en jeu, les traitements qui peuvent être effectués sur ces données, les conséquences potentielles pour les personnes concernées et les mesures de protection appropriées ;
- exercices de mise en pratique : les apprenants peuvent être invités à mettre en pratique les connaissances acquises sur les grands principes de la protection des données personnelles en effectuant des exercices pratiques tels que la rédaction d'une politique de protection des données personnelles, la réalisation d'un audit de protection des données personnelles ou la mise en place d'un plan de gestion des incidents de sécurité ;
- jeux de rôle : les jeux de rôle peuvent être utilisés pour mettre en pratique les connaissances acquises sur les grands principes de la protection des données personnelles en simulant des situations dans lesquelles les participants doivent agir en tant que responsable de traitement, sous-traitant ou personne concernée ;
- étude de cas : les études de cas peuvent être utilisées pour vérifier la compréhension des grands principes de la protection des données personnelles en examinant des situations réelles où des données personnelles ont été collectées, traitées ou utilisées de manière illégale. les apprenants doivent ensuite identifier les mesures de protection appropriées pour éviter ces violations ;
- réalisation d'un tableau de liaison entre les principes, et les obligations ou les droits des personnes concernées.

4. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- les obligations envers les personnes concernées :

    - ✓ l'obligation d'information : définition, base légale, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ le consentement définition (éclairé, spécifique) principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ l'obligation d'assurer la confidentialité et la sécurité des données : définition, fondement, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ l'obligation de pérennité et l'obligation de conservation : définitions, bases légales, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ l'obligation de respecter la finalité : définition, base légale, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ l'obligation de respecter les droits des personnes concernées : définition, base légale, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ l'obligation de tenir un registre des traitements de données : définition, base légale, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs.

- les obligations envers l'Autorité :

    - ✓ l'obligation de formalités préalables définition, base légale, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ l'obligation de notification des incidents de violation : définition, base légale, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ l'obligation de coopération : définition, base légale, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs ;
    - ✓ l'obligation d'établir un rapport annuel à transmettre à l'APDP : définition, base légale, principes, et exceptions, modalités de mise en œuvre et d'application par les différents acteurs.

b. Objectifs à atteindre

La formation permet de connaître et de comprendre :

- les obligations incombant aux responsables de traitement et le contenu pratique de ces obligations ;
- le principe de responsabilité conjointe ;
- appréhender le principe de durée de conservation des données de santé ;
- le principe de responsabilité (« accountability » /redevabilité) et les mesures organisationnelles, règles internes et outils de la conformité permettant de s'assurer et de démontrer que les règles relatives à la protection des données sont respectées ;
- les droits des personnes qui participent à une recherche médicale et notamment le droit à l'information avec, dans certains cas, le recueil de leur consentement, et les obligations qui en résultent pour le responsable de traitement ;
- pour les traitements de recherche médicale, les cas dans lesquels il peut être dérogé à l'obligation d'information prévue par la loi ;
- les conditions dans lesquelles un traitement de données à caractère personnel ayant pour objet l'évaluation ou l'analyse des pratiques de soins et de prévention doit être mis en œuvre pour respecter les dispositions de la loi ;
- les garanties que doit présenter à l'APDP le responsable d'un traitement ayant pour objet l'évaluation ou l'analyse des pratiques de soins et de prévention ;
- les conditions de sécurité à mettre en œuvre pour garantir la confidentialité des informations traitées par le traitement considéré.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 9 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- étude de cas : les apprenants peuvent être soumis à une étude de cas qui met en évidence les obligations des responsables de traitement en matière de protection des données personnelles, tels que la nécessité d'obtenir le consentement des personnes concernées, de mettre en place des mesures de sécurité adéquates, de tenir un registre des activités de traitement, etc. Les apprenants doivent ensuite identifier les obligations qui sont applicables dans cette situation spécifique ;
- questions ouvertes : les apprenants peuvent être invités à répondre à des questions ouvertes portant sur les obligations des responsables de traitement en matière de protection des données personnelles. Ces questions peuvent porter sur les principaux concepts juridiques tels que la base légale du traitement, les droits des personnes concernées, les mesures de sécurité, etc.
- examen écrit : les apprenants peuvent être soumis à un examen écrit portant sur les obligations des responsables de traitement en matière de protection des données personnelles. Les questions peuvent porter sur les principaux concepts juridiques tels que la base légale du traitement, les droits des personnes concernées, les mesures de sécurité, etc.
- QCM (questionnaire à choix multiples) : il est possible de poser des questions à choix multiples portant sur les obligations des responsables de traitement en matière de

protection des données personnelles. Cela permet de vérifier la connaissance des apprenants sur les différentes obligations qui incombent aux responsables de traitement.

5. TIERS DESTINATAIRES ET SOUS TRAITANTS

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- définition et base légale de la sous traitance ;
- rôle et distinction fonctionnelle ;
- statut, Régime juridique et responsabilité ;
- définitions des notions de tiers, destinataires en matière de protection des données personnelles ;
- les obligations des responsables de traitement en matière de protection des données personnelles vis-à-vis des tiers, destinataires et sous-traitants ;
- les différentes bases légales permettant de communiquer des données personnelles à des tiers, destinataires ou sous-traitants, tels que le consentement de la personne concernée, l'exécution d'un contrat, le respect d'une obligation légale, etc.
- les mesures de sécurité et les garanties à mettre en place pour assurer la protection des données personnelles communiquées à des tiers, destinataires ou sous-traitants ;
- les obligations spécifiques incombant aux sous-traitants en matière de protection des données personnelles, tels que la conclusion d'un contrat de sous-traitance, la mise en place de mesures de sécurité adéquates, la coopération avec le responsable de traitement, etc.
- les conséquences en cas de non-respect des obligations en matière de tiers, destinataires et sous-traitants, telles que les sanctions administratives, les actions en responsabilité civile, etc.
- les bonnes pratiques à adopter pour gérer efficacement les relations avec les tiers, destinataires et sous-traitants en matière de protection des données personnelles.

b. Objectifs à atteindre

La formation permet de connaître et de comprendre :

- les différentes obligations et les bonnes pratiques à mettre en place pour gérer efficacement les relations avec les tiers, destinataires et sous-traitants dans le cadre du régime de protection des données personnelles ;
- les différentes obligations des responsables de traitement en matière de protection des données personnelles vis-à-vis des tiers, destinataires et sous-traitants ;
- et d'identifier les différentes bases légales permettant de communiquer des données personnelles à des tiers, destinataires ou sous-traitants ;
- les mesures de sécurité et les garanties à mettre en place pour assurer la protection des données personnelles communiquées à des tiers, destinataires ou sous-traitants ;
- les obligations spécifiques incombant aux sous-traitants en matière de protection des données personnelles ;
- savoir évaluer les risques liés à la communication de données personnelles à des tiers, destinataires ou sous-traitants, et mettre en place des mesures adéquates pour y faire face.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 7 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- examen écrit: il peut s'agir d'un examen sous forme de questions à choix multiples ou de questions ouvertes qui permettent de vérifier si les apprenants ont assimilé les concepts et les bonnes pratiques abordés dans la formation ;
- rédaction juridique d'accord de confidentialité et clause de responsabilité ;
- études de cas qui permettent aux apprenants de mettre en pratique leurs connaissances sur les obligations des responsables de traitement vis-à-vis des tiers, destinataires et sous-traitants en matière de protection des données personnelles ;
- travaux pratiques et simulation de situations qui permettent aux apprenants de mettre en place des mesures de sécurité et des garanties pour assurer la protection des données personnelles communiquées à des tiers, destinataires ou sous-traitants ou d'appliquer les bonnes pratiques et les mesures de sécurité en matière de tiers, destinataires et sous-traitants ;
- quiz interactifs pour évaluer les connaissances des apprenants en temps réel et leur permettre de s'auto-évaluer.

6. STATUT, ROLE ET OBLIGATIONS DU DELEGUE A LA PROTECTION DES DONNEES PERSONNELLES (DPDP)

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- définition et base légale ;
- rôle et distinction fonctionnelles (Responsable de traitement, RSSI, etc..) ;
- obligations du délégué à la protection des données personnelles ;
- statut, Régime juridique et indications de profil ;
- modalités de désignation du DPDP.

b. Objectifs à atteindre

La formation permet de comprendre et de connaître :

- les cas de désignation obligatoire d'un délégué à la protection des données et les différents types et modalités de désignation ;
- l'expertise et les compétences attendues du délégué à la protection des données ;
- les fonction et missions du délégué à la protection des données ;
- le rôle du délégué à la protection des données dans la tenue du registre ;
- le rôle du délégué à la protection des données dans l'étude des risques ;
- les relations entre l'APDP et le délégué à la protection des données ;
- les conditions et la procédure relative à la fin de mission du délégué à la protection des données ;
- le statut du délégué à la protection des données et les différents types de désignation;
- les modalités et la procédure de désignation du délégué à la protection des données;
- les conditions dans lesquelles la liste des traitements doit être tenue par le délégué à la protection des données ;
- les conditions dans lesquelles le délégué à la protection des données participe au traitement des réclamations adressées au responsable des traitements ;
- les conditions dans lesquelles le délégué à la protection des données doit établir le bilan annuel de son activité ;
- les conditions dans lesquelles le délégué alerte le responsable de traitement sur les manquements qu'il constate.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 6 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- étude de cas pratiques qui permettent aux apprenants de mettre en pratique leurs connaissances sur le rôle et les responsabilités du DPDP/DPO en matière de protection des données personnelles ou des travaux pratiques qui permettent aux apprenants de mettre en place des mesures de sécurité et de garanties pour assurer la protection des données personnelles, ainsi que de gérer les demandes des personnes concernées ;
- note écrite de questions à choix multiples ou de questions ouvertes pour évaluer les connaissances des apprenants sur les obligations et le rôle du DPDP ;
- quiz interactifs pour évaluer les connaissances des apprenants en temps réel et leur permettre de s'auto-évaluer.

7. DROITS DES PERSONNES CONCERNEES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- définition et base légale de la notion de personne concernée en général ;
- le droit d'accès : définition, base légale, modalité de mise en œuvre, exception ;
- le droit de rectification et de suppression : définition, base légale, modalité de mise en œuvre en matière, exception ;
- le droit à réparation et responsabilité : définition, base légale, modalité de mise en œuvre, exception ;
- le droit à l'oubli : définition, base légale, modalité, de mise en œuvre, exception ;
- le droit de saisir l'APDP et d'agir contre son inaction **:** définition, base légale, modalité de mise en œuvre ;
- le droit d'opposition : définition, base légale, modalité de mise en œuvre, exception ;
- le droit d'interrogation : définition, base légale, modalité de mise en œuvre, exception ;
- le droit à la portabilité des données : définition, base légale modalités de mise en œuvre, exception ;
- prise de décision automatisée, y compris le profilage, limitations.

b. Objectifs à atteindre

La formation permet de comprendre et de connaître :

- le droit à l'information des personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement ;
- le droit d'opposition des personnes, les modalités de son exercice et les obligations qui en résultent pour le responsable de traitement ;
- le droit d'accès dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement ;
- le droit de rectification et de suppression dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 5 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- QCM (questionnaire à choix multiples) : il peut être utilisé pour évaluer les connaissances des apprenants sur les droits des personnes concernées. Les

questions peuvent porter sur des notions juridiques, des règlementations, des pratiques de protection des données, etc.

- étude de cas : les participants peuvent être invités à analyser et à résoudre des cas pratiques impliquant les droits des personnes concernées. Ils peuvent être évalués sur leur capacité à identifier les problèmes de confidentialité, à proposer des solutions pour les résoudre, etc.
- examens pratiques : les participants peuvent être évalués sur leur capacité à appliquer les connaissances acquises dans des situations pratiques, telles que des scénarios de gestion des données personnelles ou de protection de la vie privée.

8. OPERATIONS DE TRAITEMENT ET CADRE JURIDIQUE DE TRAITEMENT DES DONNEES PERSONNELLES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- définition du traitement de données personnelles ;
- définition des différentes opérations de traitement ;
- les bases juridiques de traitement des données personnelles ;
- les dérogations et spécificités.

Les exigences de conformité :

- les conditions de licéité des traitements de données personnelles de santé ;
- de finalité du traitement ;
- de proportionnalité du traitement au regard de la finalité ;
- de minimisation des données collectées au regard de la finalité ;
- de sécurité des données collectées ;
- de durée de conservation des données collectées ;
- de destinataires des données collectées ;
- d'encadrement des relations avec les sous-traitants ;
- d'information claire et préalable des personnes concernées ;
- de conditions d''exercice des droits des personnes ;
- et le cas échéant, l'encadrement des transferts de données.

Les régimes juridiques de formalités préalables :

- la déclaration : définition, traitements soumis à déclaration ;
- l'autorisation : définition, traitements soumis à l'autorisation ;
- le code de conduite : définition, traitements soumis à l'autorisation ;
- les règles d'entreprises contraignantes ou BCR : définition, modalités de mise en œuvre ;
- l'avis : définition, traitements soumis à l'avis.

b. Objectifs à atteindre

La formation permet de connaître et de déterminer :

- les différences entre traitements et opérations de traitements ;
- les différentes opérations de traitement de données ;
- le régime des formalités préalables applicable aux traitements de données ;
- les modalités juridiques de mise en conformité des traitements ;
- le contenu du dossier de mise en conformité.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 8 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- analyse d'un cas concret : les participants peuvent être invités à analyser un cas concret impliquant une opération de traitement de données personnelles. Ils pourraient être évalués sur leur capacité à identifier les problèmes juridiques et à proposer des solutions en fonction du cadre juridique en vigueur ;
- quiz : les apprenants pourraient être évalués à l'aide d'un quiz portant sur les notions clés du cadre juridique et les opérations de traitement de données personnelles. Les questions pourraient porter sur les différents types de données personnelles, les obligations légales, les sanctions encourues en cas de non-respect des règles, etc.
- rédaction de documents : les participants sont invités à remplir les formulaires de demande ou rédiger des documents tels que des notices d'information ou des politiques de confidentialité. Ils pourraient être évalués sur leur capacité à identifier les informations essentielles à inclure dans ces documents en fonction des obligations légales en vigueur.

9. COMMUNICATION ET TRANSFERT DE DONNEES PERSONNELLES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- notion de communication de données ;
- notion de transfert de données ;
- les différents types de transferts de données ;
- les types de communication de données ;
- les bases juridiques de la communication ou du transfert de données ;
- motifs d'interdiction, juridictions appropriées, Safe Harbor et Privacy Shield, clauses ;
- contractuelles types, règles d'entreprise contraignantes (BCR), codes de conduite et certifications, dérogations, évaluations de l'impact du transfert (TIA) ;
- les obligations en matière de communication et de transfert de données ;
- l'équivalence des conditions de protection des données personnelles avec le for
- les garanties et mesures juridiques dans le cadre d'un transfert ou d'une communication de données ;
- les bonnes pratiques en matière de communication et de transfert de données ;
- clauses contractuelles types ;
- Boite à outils de l'APDP.

b. Objectifs à atteindre

L'accent sera spécifiquement mis sur :

- les enjeux de la gouvernance des données et de la protection des données personnelles ;
- les risques liés à la communication et au transfert de données ;
- la sécurité de la communication et du transfert de donnée personnelle ;
- la responsabilité des acteurs impliqués dans une communication ou un transfert de données ;
- les périmètres géographiques de la communication et du transfert de données ;
- la conformité du destinataire des données ;
- l'équivalence des conditions de protection des données.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 6 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- mise en œuvre d'une grille de comparaison législative ;

- quiz : un quiz peut être administré pour évaluer les connaissances des apprenants sur les concepts clés liés à la communication et au transfert de données personnelles. Les questions peuvent porter sur des notions juridiques, des règlementations, des pratiques de protection des données, etc.
- étude de cas : les apprenants peuvent être invités à analyser et à résoudre des cas pratiques impliquant la communication et le transfert de données personnelles. Ils peuvent être évalués sur leur capacité à identifier les problèmes de confidentialité, à proposer des solutions pour les résoudre, etc.
- examens pratiques : les apprenants peuvent être évalués sur leur capacité à appliquer les connaissances acquises dans des situations pratiques, telles que des scénarios de communication ou de transfert de données personnelles.

10. NOTION DE FINALITE DU TRAITEMENT ET CARTOGRAPHIE DES TRAITEMENTS

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- définitions et finalités ;
- essai de synthèse des finalités ;
- les catégories de données de santé ;
- présentation des dispositifs législatifs et réglementaires d'encadrement de l'exercice des différentes professions de santé ;
- essai de cartographie des traitements.

b. Objectifs à atteindre

L'accent sera spécifiquement mis sur :

- la notion finalité dans chaque secteur de santé ou connexe à la santé ;
- sur le principe de la limitation de la finalité ;
- la cartographie des compétences : l'énumération exhaustive des dispositions législatives et règlementaires et les compétences que ces dispositions confèrent à chaque secteur d'activités pour le traitement des données de santé :

    - ✓ Domaine ;
    - ✓ Prérogatives ;
    - ✓ Services.

- la cartographie des données : il s'agit de faire la liste des catégories (les grands ensembles) puis de dresser le détail de chaque catégorie ;
- la cartographie des traitements des données personnelles (méthodologie et contenus) ;
- les finalités du traitement, le ou les acteurs internes du traitement des données personnelles, les intervenants extérieurs, le ou les sous-traitants, la communication des données ; le transfert.

La formation permet de connaître et de déterminer :

- le contenu du registre d'activités de traitement (responsable de traitement), du registre des catégories d'activités de traitement (sous-traitant) et du registre des violations de données ;
- la méthodologie d'élaboration d'une cartographie ;
- les éléments essentiels de la cartographie.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 6 heures.

d. Évaluation des acquis

Il peut être proposé uniquement ou conjointement un ou plusieurs exercices suivants :

- QCM (questionnaire à choix multiples) : un questionnaire à choix multiples peut être utilisé pour évaluer la compréhension des concepts clés, tels que les finalités légitimes, les catégories de données personnelles, les destinataires des données, etc.
- étude de cas : les apprenants peuvent être invités à analyser des cas pratiques impliquant la collecte et l'utilisation de données personnelles dans des contextes professionnels. Ils peuvent être évalués sur leur capacité à identifier les finalités légitimes, à évaluer les risques pour les droits et libertés des personnes concernées, à cartographier les traitements de données, etc.
- examens pratiques : les apprenants peuvent être évalués sur leur capacité à appliquer les connaissances acquises dans des situations pratiques, telles que la rédaction d'une cartographie des traitements de données dans leur organisation, la réalisation d'un registre des activités de traitement des données personnelles.

11. ASPECTS ORGANISATIONNELS DE LA CONFORMITE EN MATIERE DE PROTECTION DES DONNEES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- les mesures juridiques :

  - ✓ le code de conduite : définition, traitements soumis à l'autorisation ;
  - ✓ les règles d'entreprises contraignantes ou BCR : définition, modalités de mise en œuvre ;
  - ✓ le règlement de traitement ;
  - ✓ documentations et processus.

- les mesures de sécurité (la Politique de Sécurité des Systèmes d'Information – PSSI, Niveaux de confidentialité des données (pseudonymisation, anonymisation, chiffrement, etc…) ;
- les mesures techniques : l'identification et authentification, la lutte contre les intrusions extérieures dans le réseau (firewall, anti-virus), La protection via des flux sécurisés (TSL/SSL, https, sftp) ;
- les mesures physiques ;
- les mesures logiques ;
- les mesures organisationnelles (cartographie des données, Déploiement d'une solution de data management, Revue des contrats (sous-traitants, partenaires, salariés, clients), Sensibilisation/formation des équipes métiers et IT, Tenue du registre des activités de traitement, Politique de minimisation des données (Privacy by design), analyse de risque (PIA/EIVP) ;
- principes éthiques des professionnels de la protection des données personnelles ;
- présentation de la boite à outils de l'APDP.

b. Objectifs à atteindre

- l'accent sera spécifiquement mis sur les aspects et l'organisation pratique de la protection ;
- les mesures à mettre en place pour utiliser et exploiter les données de santé ;
- les modalités d'information appropriées ;
- les conseils pour adopter les bonnes pratiques.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 6 heures.

d. Évaluation des acquis

- évaluation théorique : examen écrit, QCM, quizz ou réponses écrites à des questions ouvertes sur les types de mesure organisationnelles, les politiques et procédure de protection des données, principes de protection des données personnelles, les réglementations en vigueur et les méthodologies d'analyse d'impact, les étapes clés de l'analyse d'impact ou de citer les principaux risques liés au traitement des données personnelles ;
- test pratique : réaliser une analyse d'impact pour un scénario de cas pratique peut aider à évaluer la capacité à appliquer les principes et les méthodologies d'analyse d'impact dans un contexte réel.

12. ANALYSE D'IMPACT POUR LA PROTECTION DES DONNEES PERSONNELLES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- les étapes de la gestion des risques (identification, impact potentiel, contexte, etc…) ;
- principes et processus clés de l'analyse d'impact ;
- les conditions d'exigence de l'analyse d'impact en matière de données sensibles ;
- les principaux diagnostics à mener dans un audit (L'audit des dispositifs de collecte des données, L'audit du système d'information, l'audit des traitements, L'audit de sécurité (identification et définition des types de risques, hiérarchisation ;
- l'évaluation du niveau de sécurité (guide d'audit, systèmes informatiques, processus et flux de données impliqués dans le traitement des données personnelles, etc.) ;
- outils préventifs et correctifs de gestion des risques ou incidents en matière de traitement des données de santé.

b. Objectifs à atteindre

La présentation doit permettre aux participants de comprendre la nécessité de réaliser une analyse d'impact, l'utilité de ces démarches dans les formalités préalables, la gestion des incidents, les outils d'audit et de gestion de risque, de veiller à l'efficacité et à la pérennité desdits outils (éviter d'utiliser des outils obsolètes).

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 8 heures.

d. Évaluation des acquis

- évaluation théorique : examen écrit, QCM, quizz ou réponses écrites à des questions ouvertes sur les principes de protection des données personnelles, les réglementations en vigueur et les méthodologies d'analyse d'impact, les étapes clés de l'analyse d'impact ou de citer les principaux risques liés au traitement des données personnelles ;
- test pratique : réaliser une analyse d'impact pour un scénario de cas pratique peut aider à évaluer la capacité à appliquer les principes et les méthodologies d'analyse d'impact dans un contexte réel.

13. SECURISATION DES DONNEES PERSONNELLES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- rappels :
  - ✓ obligations du responsable de traitement ;
  - ✓ droits des personnes concernées ;
  - ✓ distinction sécurisation du système d'information et sécurisation des données et du traitement.
- sécurité by design ;
- principes de sécurité appliqués aux traitements manuels et aux traitements automatisés ;
- catégories de sécurité (technique, organisationnelle) ;
- principales mesures de sécurité ;
- fonctions du RSSI ;
- mesures de sécurité opérationnelles :

  - ✓ gestion des accès, identification, authentication ;
  - ✓ classification et chiffrement ;
  - ✓ sécurité des échanges ;
  - ✓ anonymisation et pseudonymisation ;
  - ✓ accès/requêtes tracés ;
  - ✓ sécurisation du hardware et du software ;
  - ✓ hébergement de données et d'Entrepôt de Données ;
  - ✓ mutualisation de la conservation et du stockage.

b. Objectifs à atteindre

La formation permet :

- de s'approprier des notions de sécurité, de confidentialité et des conditions de leur mise en œuvre et de leur actualisation ;
- de connaître et de déterminer les risques attachés à la protection des données personnelles ;
- de connaître et de déterminer l'intérêt d'un plan de sécurité et d'une politique de sécurité des systèmes d'information ;
- les modalités de mise en œuvre d'un plan de sécurité et d'une politique de sécurité des systèmes d'information ;
- identifier et indiquer les mesures de sécurité (la Politique de Sécurité des Systèmes d'Information – PSSI, Niveaux de confidentialité des données (pseudonymisation, anonymisation, chiffrement, etc…) et les mesures techniques : l'identification et authentification, la lutte contre les intrusions extérieures dans le réseau (firewall, anti-virus), La protection via des flux sécurisés (TSL/SSL, https, sftp) ;

- de déterminer et décrire les règles de sécurité informatique s'appliquant à la donnée de santé (chiffrement…) ;
- de présenter les méthodes d'anonymisation des données personnelles ;
- gérer la sécurité des communications de données, transfert de données ;
- de connaitre et comprendre les enjeux, les objectifs, les avantages, les inconvénients du stockage et de la mutualisation des données de santé.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 8 heures.

d. Évaluation des acquis

- évaluation en continu : Vous pouvez évaluer la compréhension des apprenants tout au long de la formation en leur demandant de réaliser des exercices pratiques, des quiz ou des travaux écrits. Cela vous permettra d'identifier les lacunes et les points forts des apprenants au fur et à mesure de la formation ;
- Questionnaire à Choix Multiple (QCM) : Vous pouvez créer un questionnaire à choix multiple portant sur les notions abordées pendant la formation. Les questions peuvent porter sur des notions comme les types de données personnelles, les méthodes de sécurisation, les risques liés à la protection des données personnelles, etc.
- étude de cas : Vous pouvez soumettre une étude de cas à résoudre, dans laquelle les apprenants doivent identifier les risques de sécurité des données personnelles et proposer des solutions pour les minimiser ;
- simulation de piratage : Vous pouvez organiser une simulation de piratage pour tester les compétences techniques des apprenants dans la protection des données personnelles. Vous pouvez leur demander de détecter les vulnérabilités et de proposer des solutions pour y remédier ;
- présentation orale : Vous pouvez demander aux apprenants de préparer une présentation orale sur un sujet lié à la sécurisation des données personnelles, comme les enjeux de la protection des données ou les méthodes de sécurisation. La présentation peut être suivie d'une séance de questions-réponses pour évaluer leur compréhension du sujet.

14. REGULATION ET CONTROLE DU REGIME DE PROTECTION DES DONNEES PERSONNELLES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- l'Autorité de Protection des données personnelles ;
- pouvoir de régulation de l'APDP ;
- pouvoir de contrôle de l'APDP ;
- éléments de contrôle/d'audit de conformité ;
- modalités de mise en œuvre des contrôles (à distance, sur site, opérationnelle, documentaire, etc.) ;
- les droits des responsables de traitement pendant le contrôles, vérifications et visites ;
- les différents acteurs du contrôle ;
- les actes conservatoires ;
- le contentieux du contrôle.

b. Objectifs à atteindre

La formation permet également de comprendre et de connaître :

- l'Autorité de Protection des Données Personnelles ;
- les différentes formes de contrôles a posteriori pouvant être effectués par l'APDP ;
- les conditions dans lesquelles un délit d'entrave à l'action de l'APDP est constitué ;
- le formalisme associé à une procédure de contrôle ;
- les modalités pratiques d'exercice d'une procédure de contrôle ;
- comment mettre en œuvre les droits et les obligations du responsable de traitements dans le cadre d'une procédure de contrôle ;
- les suites consécutives à un contrôle ;
- les différentes procédures de sanction pouvant être mises en œuvre par l'APDP ;
- le fonctionnement de la plénière réunie en formation contentieuse et le déroulement d'une séance ;
- le formalisme associé à une procédure de sanction, les droits et les obligations du responsable de traitement mis en cause et les voies de recours ;
- les conditions de publication et de publicité des sanctions.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 6 heures.

d. Évaluation des acquis

- évaluation des connaissances théoriques : vous pouvez créer un quiz ou un test écrit qui couvre les notions théoriques du régime de protection des données personnelles,

telles que les définitions clés, les droits des personnes concernées, les obligations des responsables de traitement et des sous-traitants, les mécanismes de conformité et les sanctions en cas de non-respect ;

- étude de cas : vous pouvez soumettre une étude de cas pratique pour évaluer la capacité des apprenants à appliquer les principes du régime de protection des données personnelles dans des situations réelles. Les apprenants devront identifier les problèmes de conformité et proposer des solutions pour y remédier ;
- examen oral : vous pouvez organiser un examen oral individuel ou en groupe où les apprenants présentent leur compréhension du régime de protection des données personnelles et leur capacité à appliquer les principes dans des scénarios pratiques ;
- simulations de conformité ou de contrôle : vous pouvez organiser des simulations de conformité pour tester les compétences des apprenants dans des situations réelles et mesurer leur aptitude à mettre en place des process.

15. SANCTIONS DES MANQUEMENTS ET VIOLATIONS DU REGIME DE PROTECTION DES DONNEES PERSONNELLES

a. Points à couvrir par la présentation

La formation permet de couvrir les points suivants :

- les sanctions de la compétence de l'APDP :
  - ✓ mesures administratives, base légale, avertissement, mise en demeure, injonction, retrait d'autorisation, le verrouillage de données ; les procédures de mise en œuvre ;
  - ✓ les sanctions pécuniaires : base légale, procédures de mise en œuvre.
- présentation des dispositions pénales associées au non-respect de la loi ;
- les sanctions de la compétence des juridictions :
  - ✓ la responsabilité civile : le principe, le régime ;
  - ✓ la responsabilité pénale : les incriminations, la répression.

b. Objectifs à atteindre

La formation permet enfin de comprendre et de connaître :

- les sanctions pénales liées au non-respect des exigences relatives au caractère loyal et licite de la collecte de données ;
- les sanctions pénales relatives aux atteintes aux droits d'accès, de rectification ou d'opposition de la personne ;
- les sanctions pénales liées au non-respect des exigences relatives à l'information des personnes ;
- les sanctions pénales liées au non-respect des exigences relatives aux formalités préalables ;
- les sanctions pénales liées au non-respect des exigences relatives à la sécurité des données ;
- les sanctions pénales liées au non-respect des exigences relatives à la durée de conservation des données ;
- les sanctions pénales liées au non-respect de la finalité des traitements ;
- les sanctions pénales liées au non-respect des exigences relatives au traitement des données sensibles.

c. Durée de la formation

Cette formation est organisée sur une durée minimale de 5 heures

d. Évaluation des acquis

- auto-évaluation : les participants peuvent s'auto-évaluer en faisant une analyse critique de leur compréhension des différents aspects de la réglementation en vigueur en

matière de protection des données personnelles, ainsi que sur les différentes sanctions prévues en cas de manquements et violations ;

- examen écrit : les participants peuvent être soumis à un examen écrit portant sur les différentes sanctions prévues par la réglementation en vigueur en cas de manquements et violations du régime de protection des données personnelles. L'examen peut comporter des questions ouvertes et fermées, ainsi que des études de cas ;
- étude de cas : les participants peuvent être invités à résoudre des cas pratiques portant sur des manquements et violations du régime de protection des données personnelles. Ces cas peuvent être basés sur des situations réelles ou fictives, et doivent permettre aux participants de mettre en pratique les connaissances acquises pendant la formation ;
- simulation de procédure disciplinaire : les participants peuvent être invités à simuler une procédure disciplinaire pour violation du régime de protection des données personnelles. Cette simulation doit permettre aux participants de comprendre les différentes étapes de la procédure, ainsi que les rôles et responsabilités des différents acteurs impliqués ;
- évaluation par un expert ou APDP : les participants peuvent être évalués par un expert en la matière, qui pourra poser des questions sur les différents aspects de la réglementation en vigueur en matière de protection des données personnelles, ainsi que sur les différentes sanctions prévues en cas de manquements et violations. L'expert peut être désigné par l'APDP à la demande de l'organisme de formation. Les participants peuvent être confrontées à la plateforme d'évaluation de l'APDP.