Catalogue de formations 2024

Protection des données, Vie privée, Droit de la cybersécurité

HS2
Hervé Schauer Sécurité

SOMMAIRE ET CALENDRIER

***Examen de certification HS2 inclus**
***Examen de certification AFNOR certification inclus**

Formation
« RGPD : les fondamentaux de la protection des données »

Réf : RGPD

Le mot « RGPD » est sur toutes les lèvres depuis l'entrée en application, il y a plus d'un an, du règlement général n°2016/679 sur la protection des données. Les principes directeurs de la conformité et les principaux points d'achoppement du texte apparaissent aujourd'hui. Projet transversal et pluridisciplinaire qui implique tous les collaborateurs de l'entreprise, le RGPD est difficile de lecture et d'application. L'objectif de cette formation courte est d'en donner une vision d'ensemble et de livrer ses notions clés. Elle délivre la base de connaissance nécessaire pour traiter les questions récurrentes et prendre part aux projets comprenant des données personnelles.

Objectifs

- Connaître le règlement et les évolutions apportées par celui-ci
- Avoir une vision d'ensemble de la protection des données personnelles
- Maîtriser les notions clés du RGPD et comprendre ses implications opérationnelles

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Chef de projet
- RSSI, DSI
- Directions
- Juriste
- Consultant en protection des données
- DPO, DRPO et futur DPO

Pré-requis

- Aucun pré-requis n'est demandé cependant avoir des bases informatique ou juridiques est un plus.

Méthode pédagogique

- Cours magistral avec exemples et échanges interactifs.

Supports

- Support de cours au format papier en français
- Tous les documents nécessaires à la formation en français ou anglais dont le texte du règlement et certaines lignes directrices du CEPD
- Certificat attestant de la participation à la formation
- Certificat de réussite de l'examen final

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification RGPD par HS2.**

Programme

Introduction

- Fondamentaux juridiques
- Historique et avenir du règlement européen
- Enjeux de la protection des données à caractère personnel (DCP)

Fondamentaux de la protection des données

- Champ d'application du règlement
- Principes fondamentaux
- Privacy by Design, Privacy by default
- Notions essentielles et acteurs
- Données à caractère personnel, traitement, etc.
- Autorités de protection des données
  - CNIL
    - Pouvoirs
    - Guichet unique
  - Contrôle
- Comité Européen à la Protection des Données (CEPD)
- DPO (Délégué à la Protection des Données)
- Responsabilités
  - Responsabilité du DPO
    - Responsabilité du sous-traitant
    - Responsabilité conjointe
    - Autres cas
    - Sanctions

Missions du responsable de traitement et du sous-traitant

- Désigner un DPO
- Réaliser une analyse d'impact sur les DCP (PIA : Privacy impact assessment)
- Consulter au préalable l'autorité de contrôle
- Tenir un registre des activités de traitements
- Veiller aux données particulières (données sensibles, judiciaires, protection des mineurs, santé, etc.)
- Assurer la sécurité des données
- Évaluation du niveau de sécurité
- Mesures techniques et organisationnelles
- Violations de données personnelles
- Gérer les droits des personnes concernées
- Transparence et information
- Droit d'accès
- Droit de rectification et effacement (droit à l'oubli numérique)
- Droit à la limitation du traitement
- Droit à la portabilité
- Droit d'opposition
- Veiller aux transferts de données en dehors de l'UE
- Se préparer à un contrôle
- Coopérer avec les autorités

Outils

- Certifications et labels
- Codes de conduite et chartes
- Check-list
- Veille
- Références

Formation « Métier de DPO »

Pratiques et Échanges entre professionnels

Réf : DPO

La formation Métier de DPO est dédiée aux DPO (ou délégués à la protection des données) et à toute personne en charge de la protection de la vie privée.
L'objectif de la formation est de permettre aux professionnels de la protection des données d'échanger entre eux et d'adresser leurs questions tant juridiques et pratiques aux formateurs.
L'approche de cette formation se veut opérationnelle et pragmatique. Ainsi, son programme prend la forme d'un plan d'action du DPO.

Objectifs

- **Connaître le métier de DPO : ses missions, ses responsabilités et son positionnement**
- **Créer un espace d'échanges entre professionnels de la protection des données**
- **Présenter un plan d'action pour un DPO fraîchement nommé**
- **Réaliser des focus sur les sujets complexes régulièrement rencontrés par les DPO**

Durée & horaires

- **5 jours, soit 35h00**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants.**

Public visé

- **DPO**
- **Adjoints au DPO**
- **Relais ou référents informatique et libertés**
- **Consultants conseils en protection des données**
- **Et plus généralement toute personnes ayant une expérience en matière de protection des données et souhaitant approfondir ses connaissances métier**

Pré-requis

- **Avoir une bonne expérience professionnelle dans le secteur de la protection des données**
- **Connaître les exigences légales et réglementaires applicables en la matière**

Méthode pédagogique

- **Une formation construite sous l'angle d'un plan d'action du DPO**
- **Une présentation des exigences légales et réglementaires, des enjeux opérationnels qui en découlent et des retours d'expérience des formateurs ainsi que des participants**
- **Des focus sur les sujets de droit complexes régulièrement rencontrés par les DPO**
- **Des exercices pratiques individuels ou en groupe effectués par les stagiaires, basés sur des études de cas, permettant de se confronter à des situations réelles**
- **La création d'un espace d'échange entre professionnels de la protection des données**

Supports

- **Support de cours au format papier en français ;**
- **Cahier d'exercices et corrections des exercices ;**
- **Feuilles d'émargement par demi-journée de formation et certificat individuel de formation attestant de la participation à l'ensemble de la formation.**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.**

Certification

- **Cette formation n'est pas certifiante.**

Programme

0 – Introduction

1 – Je décroche un poste de DPO

1.1 – Mon statut
1.2 – Mes compétences
1.3 – Mon positionnement
1.4 – Mes missions
1.5 – Ma prise de fonctions

2 – Je prends mes fonctions, j'identifie l'existant

2.1 – Identifier l'existant et Définir le contexte
2.2 – Gérer un projet

3 – Je pilote la cartographie des traitements

3.1 - Dresser le registre des activités de traitement
3.2 - Identifier les traitements critiques et comprendre leur écosystème

4- Je me présente et j'instaure les bons réflexes

4.1 – Former, sensibiliser et communiquer
4.2 – Déployer les premiers processus prioritaires

5 – J'attaque la mise en conformité de l'existant, je priorise les actions

5.1 - Priorisation et plan d'action
5.2 - Mise en conformité des traitements
5.3 - Gérer les droits des personnes et les réclamations
5.4 - Gérer les partenaires

6 - Je gère les risques sur la vie privée et les mesures de sécurité associées

6.1 - Réaliser les PIA
6.2 - Assurer la sécurité des données
6.2.1 La sécurité, une approche par le risque
6.2.2 Gestion des incidents
6.2.3 Surveillance et amélioration continue

7 – La gouvernance de la protection des données

7.1 - Politiques et procédures
7.2 - Suivi et communication des chantiers
7.3 - Management de la protection des données
7.4 - Opportunité de la certification ?

8 - Je me prépare à un contrôle de la CNIL

Formation « Préparation à l'examen DPO Afnor Certification »

Réf : CERTIFDPO

La formation certifiante par excellence pour obtenir la certification de Data Protection Officer (DPO) et confirmer l'étendue de vos connaissances en matière de protection des données. **Notre formation est entièrement dédiée à l'obtention de cette certification !**
Notre formation est enregistrée par AFNOR Certification comme prérequis à la certification de compétences des DPO.
AFNOR Certification est historiquement le 1er organisme certificateur agréé par la CNIL pour certifier les compétences des délégués à la protection des données / Data Protection Officer (DPO), sur la base des référentiels du 20 septembre 2018 adoptés par la CNIL.

ATTENTION : Pour une formation permettant de s'approprier les démarches et les outils dédiés à la protection des données, approfondir ses connaissances du métier du DPO et apprendre à gérer la conformité RGPD de son organisation, nous vous recommandons plutôt la formation « Métier du DPO » qui répondra à toutes ces attentes.

Objectifs

- **Acquérir les connaissances juridiques, techniques et organisationnelles nécessaires à la réussite à l'examen de certification.**

Durée & horaires

- **5 jours, soit 37h heures réparties en 35h00 de cours (dont 2h de travail personnel) et 2h d'examen.**
- **Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 16h00/16h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 16 participants.**

Public visé

- **Personnes ayant à prendre en charge ou à mettre en œuvre la conformité de traitements de données personnelles à tous les niveaux, du management à l'opérationnel en passant par la conformité et souhaitant disposer de la certification DPO :**
  - **DPO, DRPO**
  - **Personnes responsables de services opérationnels**
  - **DSI et leurs équipes**
  - **Responsables conformité, responsables des risques**
  - **Juristes et responsables juridiques**
  - **Consultants accompagnant à la mise en conformité RGPD ou assistant le DPO**

Pré-requis

- **Avoir au minimum relu :**
  - **Les principales lignes directives du CEPD**
  - **Les principales recommandations de la CNIL**
- **Avoir passé les MOOCs de la CNIL et de l'ANSSI**
- **Avoir des bases informatiques ou juridiques est un vrai plus.**

Méthode pédagogique

La méthode pédagogique se fonde sur les quatre axes suivants :

- **Un cours magistral sur le sujet, construit en partant des textes et documents officiels mais adapté de façon à rendre la matière compréhensible en langage courant, pour appréhender au mieux les questions de l'examen**
- **Enrichi de cas pratiques et d'exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous avocats et consultants spécialistes reconnus de ces questions ou implémenteurs des normes ayant tous passés récemment l'examen**
- **Des quiz à chaque étape des points importants de la formation pour évaluer le niveau de compréhension et de connaissance, ainsi qu'un examen blanc dans les conditions de l'examen final**
- **Un cahier d'exercices et un cahier de révisions de notions de cours à travailler le soir permettant de se préparer aux questions de l'examen.**

Supports

- **Support de cours en français ;**
- **Cahier d'exercices et corrections des exercices ;**
- **Tous les documents nécessaires à la formation en français ou anglais ;**
- **Feuilles d'émargement par demi-journée de formation et certificat individuel de formation attestant de la participation à l'ensemble de la formation.**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.**

Certification

- **Cette formation prépare à l'examen de certification "Délégué à la protection des données" (DPO). Formation enregistrée par AFNOR Certification comme prérequis à la certification de compétences des DPO.**
- **A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 2h en français. L'examen est constitué d'un QCM. Cet exercice valide les compétences et les savoir-faire présentés dans la catégorie 2 de la délibération n°2018-318 du 20 septembre 2018. Les questions couvrent tous les domaines du programme figurant en annexe de la délibération n°2018-317 du 20 septembre 2018.**

Programme

1 - Les principes de la protection des données à caractère personnel

- **1.1 Les sources**
  - Evolution et mise en perspective des principes généraux applicables (loi informatique et Libertés, textes européens, genèse RGPD, droit comparé US)
  - Qu'est-ce que la CNIL ? Qu'est-ce que le CEPD ?
- **1.2 Les définitions essentielles**
  - De quoi parle-t-on ? Notions de donnée à caractère personnel, traitement, responsable de traitement/sous-traitant, etc.
- **1.3 Le champ d'application**
  - Champ d'application matériel du RGPD (la Directive 2016/680 dite Directive « Police », le secteur des télécom/commerce électronique)
  - Champ d'application territorial (l'autorité de contrôle « chef de file », les transferts de données hors UE/EEE, certifications/codes de conduite)

- **1.4 Les grands principes**
  - L'architecture complexe du RGPD
  - Les principes essentiels du RGPD (licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, etc.)
  - Conformité de l'écosystème (la qualification de responsable de traitement/sous-traitant ; accords contractuels)
  - Le registre de traitements

- **1.5 Les régimes spéciaux**
  - Les données à caractère hautement personnel, les données relatives aux condamnations pénales ou infractions, catégories particulières de données, etc.
  - Le profilage
  - Les référentiels de la CNIL

- **1.6 Les droits des personnes**
  - Droit à l'information, droit d'accès, droit de rectification, droit à l'effacement, droit d'opposition, etc.

2 - L'approche par les risques

- **2.1 Intégrer les principes de Privacy by design et by default**
  - Les 7 piliers du Privacy by design
  - A quoi servent ces principes ?
  - Les outils de mise en œuvre

- **2.2 Se donner les moyens d'assurer la sécurité**
  - Les violations de données personnelles : notion d'intégrité, de disponibilité, de confidentialité… et d'accountability
  - Les sanctions en cas de manquement à la sécurité
  - Notions de mesures de sécurité et d'adéquation aux risques
  - Exemples de mesures de sécurité et de contre-mesures pour chaque type de violation
  - Les bonnes pratiques, etc.

- **2.3 Evaluer les risques et analyser l'impact de vos traitements sur les droits et libertés fondamentales (AIPD)**
  - Qu'est-ce qu'une analyse d'impact ? Position de la CNIL
  - Contenu de l'AIPD
  - Appréciation du risque
  - Notion d'AIPD flash

- **2.4 Savoir notifier les violations de données personnelles**
  - Genèse de l'obligation de notification
  - Modalités de la notification (qui, quand, comment ?)
  - Modalités de la communication aux personnes concernées

- **2.5 Anticiper les recours et préparer un contrôle par les autorités**
  - Réclamations, recours, responsabilités
  - L'action collective, le droit à réparation
  - Se préparer à un contrôle de la CNIL (modalités, pouvoirs de la CNIL, sanctions)

3 - Mettre en œuvre la conformité

- **3.1 Nommer un DPO dans l'entreprise**
  - Qualités, profil, statut
- **3.2 Mettre en place et/ou gérer la gouvernance de protection des données**
  - DPO, contrôleur ou faiseur ?
  - Comité de pilotage, groupe de travail, etc.

- **3.3 Déployer une culture « Protection des données » dans l'entreprise**
  - Notion, intérêt et structuration du Dossier de conformité
  - Sensibilisation des personnels

- **3.4 Recenser parallèlement les outils et livrables de gouvernance**
  - Analyse de l'existant, veille globale
  - Accountability

- **3.5 Connaître son environnement et son écosystème**
  - Cartographies

Hervé Schauer Sécurité
Hervé Schauer Sécurité

Formation « Préparation au renouvellement de l'examen DPO Afnor Certification »

Réf : RECERTDPO

La formation par excellence pour réussir votre examen de re-certification AFNOR de Data Protection Officer (DPO). La certification DPO a en effet une durée de validité de 3 ans et l'obtention de l'examen de re-certification dans ce délai est indispensable au maintien de votre certification.
Notre formation a donc été pensée pour que vous puissiez l'obtenir sans délai, elle est entièrement dédiée à l'obtention de cet examen !

AFNOR Certification est historiquement le 1er organisme certificateur agréé par la CNIL pour certifier les compétences des délégués à la protection des données / Data Protection Officer (DPO), sur la base des référentiels du 20 septembre 2018 adoptés par la CNIL.

ATTENTION : Pour une formation permettant de s'approprier les démarches et les outils dédiés à la protection des données, approfondir ses connaissances du métier du DPO et apprendre à gérer la conformité RGPD de son organisation, nous vous recommandons plutôt la formation « Métier du DPO » qui répondra à toutes ces attentes.

Objectifs

- **Mettre à jour les connaissances juridiques, techniques et organisationnelles nécessaires à la réussite à l'examen de re-certification AFNOR**
- **S'entraîner au QCM de l'examen de re-certification AFNOR**

Durée & horaires

- **3 jours, soit 20 heures réparties en 18 heures de cours et 2 heures d'examen**
- **Horaires : le premier et le second jour : de 9h30 à 13h00 et de 14h00 à 18h00 // le 3eme jour : de 9h30 à 12h et de 13h30 à 16h (examen)**

Nombre de participants

- **Minimum 6 participants – Maximum 16 participants**

Public visé

Personnes ayant obtenu la certification DPO et souhaitant la renouveler, soit potentiellement :

- **DPO, DRPO**
- **Personnes responsables de services opérationnels**
- **DSI et leurs équipes**
- **Responsables conformité, responsables des risques**
- **Juristes et responsables juridiques**
- **Consultants accompagnant à la mise en conformité RGPD ou assistant le DPO**

Prérequis

- **Être titulaire d'une certification AFNOR encore en cours de validité à la date de la formation**
- **Bien connaître le texte du RGPD**
- **Avoir au minimum relu :**
  - **Les principales lignes directives du CEPD**
  - **Les principales recommandations de la CNIL**

Méthode pédagogique

La méthode pédagogique se fonde sur un mix constant entre :

- **Mise en situation pratique autour de questionnaires rédigées à la façon de l'examen de certification d'une part ;**
- **Et étude des principales évolutions ou approfondissements des thématiques dont la connaissance est nécessaire à la réussite de l'examen de l'autre.**

Ainsi, seront notamment prévus :

- **Des quizz à chaque étape des points importants de la formation pour évaluer le niveau de compréhension et de connaissance, ainsi qu'un examen blanc dans les conditions de l'examen final**
- **Un cahier d'exercices et un cahier de révisions de notions de cours à travailler le soir permettant de se préparer aux questions de l'examen.**

Formateurs

- **François Coupez**
- **Diane Rambaldini**
- **Clémence Scottez**
- **Amélie Paget**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Feuilles d'émargement par demi-journée de formation et certificat individuel de formation attestant de la participation à l'ensemble de la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de renouvellement de certification "Délégué à la protection des données" (DPO).**
- **A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 2h en français. L'examen est constitué d'un QCM. Cet exercice valide les compétences et les savoir-faire présentés dans la catégorie 2 de la délibération n°2018-318 du 20 septembre 2018. Les questions couvrent tous les domaines du programme figurant en annexe de la délibération n°2018-317 du 20 septembre 2018.**

Programme

Jour 1 matin :

- **Examen blanc de mise en situation ;**
- **Correction de l'examen ;**
- **Partage des difficultés rencontrées par les participants lors de leur première certification ;**

Enseignements à tirer de la norme présentant l'examen CNIL et points d'attention.

Jour 1 après-midi :

- **Retour sur les définitions essentielles du RGPD ;**
- **Focus sur les thématiques juridiques spécifiques se prêtant à des questions de QCM (grands principes, textes et références majeures, etc.) ;**
- **Quizz de cours et exercices (à base de QCM rédigées à la façon de l'examen de certification).**

Jour 2 matin :

- **Correction des exercices ;**
- **Focus sur les thématiques organisationnelles spécifiques se prêtant à des questions de QCM (les différents critères dans le RGPD – pour la nomination d'un DPO, pour la tenue d'un registre, pour la réalisation d'un PIA, etc.).**

Jour 2 après-midi :

- **Focus sur les principales notions en matière de cybersécurité (vocabulaire, résilience opérationnelle, etc.) ;**
- **Exercices (à base de QCM rédigées à la façon de l'examen de certification).**

Jour 3

- **Correction et nouveaux exercices (à base de QCM rédigées à la façon de l'examen de certification).**

Formation « PIA »

« Etude d'impact sur la vie privée : Quand, pourquoi, comment ? » / #EIVP #DPIA

Réf : PIA

À travers le règlement européen de protection des personnes physiques à l'égard de leurs données à caractère personnel (RGPD), s'est opéré un changement profond de paradigme. C'est toute la gouvernance des données qui se voit repenser au sein des organismes. Les responsables de traitement se retrouvent non seulement responsables de protéger ces données en adoptant des mesures adaptées mais également en charge de le prouver. L'incidence la plus directe est donc la place prépondérante que les organisations doivent donner à la gestion des risques mais également au contrôle interne. En effet, il leur revient désormais d'évaluer elles-mêmes la part de risques sur la vie privée des personnes dont elles collectent, consultent, manipulent, stockent ou encore transfèrent les données. Que les organisations soient plus ou moins favorables à cette démarche, il n'en demeure pas moins qu'elle a de fortes implications non seulement pour les personnes concernées et pour l'organisation elle-même. Reste que cela suppose qu'elle soit comprise, intégrée et réalisable par tous.

La formation ici proposée aura comme objectif fondamental de donner les clefs aux acteurs concernés pour instaurer ce changement culturel majeur dans l'organisation tant il va peser sur le futur non seulement de la responsabilité sociale de l'entreprise mais également sur son innovation et les valeurs véhiculées par elle.

La formation insistera particulièrement sur :

- **La gouvernance de la gestion des données et in fine, de la gestion des risques sur la vie privée**
- **Les enjeux de la maîtrise de son environnement, pour garantir la solidité de l'étude d'impact**
- **La nécessité de l'intégrer à tous les processus de l'entreprise comme n'importe quel autre et ainsi, d'en assurer sa prise en compte par défaut et dès le début d'un projet**

Objectifs

- **Être capable de savoir quand et pourquoi déclencher une EIVP / DPIA**
- **Déterminer un processus et une méthodologie de faisabilité d'une EIVP**
- **Connaître les prérequis indispensables à l'EIVP**

Durée & horaires

- **3 jours soit 21 heures**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Responsable de traitement / Sous-traitant**
- **Directions métiers**
- **Direction Générale**
- **DPO**
- **Comité pilotage RGPD (Juriste, Responsable marketing,…)**

Pré-requis

- **Avoir suivi en amont soit une formation sur le RGPD, soit une formation DPO.**

Méthode pédagogique

La formation en présentiel, ici proposée, repose sur 3 piliers qui en font son succès :

- **Le Savoir**
- **L'échange**
- **La mise en situation**

Les participants reçoivent la matière théorique, technique et pratique pour s'assurer la maîtrise du sujet. Le savoir transmis est reconnu et basé sur des référentiels éprouvés (Guides de la CNIL, Guidelines du G29/CEPD, Lois et règlements en vigueur, Norme ISO 29134. Les sessions sont basées sur l'interactivité pour qu'au fur et à mesure les participants puissent non seulement poser leurs questions et ainsi dissiper tout doute sur les points abordés, mais également pour partager leurs retours d'expérience. Enfin, les participants sont régulièrement mis en situation pour se tester.

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PIA par HS2.**

Programme

Introduction

- Cadre légal et réglementaire
- La protection des personnes physiques à l'égard de leurs données à caractère personnel : Nouvelle contrainte ou nouvelle économie ?
- La gestion des risques au cœur de la protection des données à caractère personnel

Éléments généraux sur l'EIVP (RGPD)

- Qui déclenche une EIVP ?
- Quand et pourquoi ? (Facteurs déclencheurs)
- Eléments obligatoires d'une EIVP

Questions essentielles

- Qu'est-ce qu'un risque ? un risque élevé ?
- Qu'est qu'un traitement ? un traitement à grand échelle ? un suivi régulier ?
- Analyse de risques sur les données et Analyse des risques sur les droits et libertés fondamentales des personnes : Quelles différences et dans quel ordre ?

Méthodologie

- Déclenchement du PIA (à quel moment ?)
- Les indispensables
  - Le Registre des traitements
  - Modélisation des processus métiers
  - Cartographie d'acteurs

- Périmètre
- Parties prenantes
- Référentiels :
  - Guides CNIL
  - G29
  - Norme ISO 29134
- Présentation de l'outil PIA élaboré par la CNIL (gratuit)
- Évaluation des risques
- Documentations associées
- Suites du PIA et cycle d'amélioration continue

L'intégralité de la formation est ponctuée de quizz et d'exercices de mise en pratique.

Formation « Hébergement des données de santé et vie privée »

Réf : SECUSANTE

Le secteur de la santé et du social est encadré par des règles spécifiques c'est pourquoi HS2 propose une formation dédiée pour couvrir ce domaine.

Objectifs

- Apprendre les exigences juridiques et de sécurité en matière de :
  - Protection des données personnelles de santé, y compris le RGPD et la loi Informatique & Libertés 3 dans le cadre de la santé
  - Hébergement des données de santé (certification HDS)
  - Interopérabilité des systèmes d'information de santé (CI-SIS)
  - Sécurité des systèmes d'information de santé (PGSSI-S, CPS, RGS, LPM, NIS)

Durée & Horaires

- 3 jours soit 21 heures
- 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participants

- Minimum 6 participants – Maximum 24 participants

Public visé

- Personnes des secteurs santé et social :
  - RSSI
  - DPO
  - Juristes
  - Toute personne confrontée à la gestion d'un système d'information de santé.

Pré-requis

- Avoir une culture générale en sécurité des systèmes d'information ou en droit est un plus mais n'est pas imposé.
- Pour les participants souhaitant apprendre la certification HDS, il convient d'avoir suivi la formation ISO27001 Lead Implementer avant la formation SECUSANTE.

Méthode pédagogique

- Cours magistral avec échanges interactifs

Supports

- Support de cours au format papier en français
- Cahier d'exercices et corrections des exercices
- Tous les documents nécessaires à la formation en français ou anglais
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUSANTE par HS2.**

Programme

Module 1 : Présentation du contexte

- Cadre légal et normatif
- Notions fondamentales
- Données de santé, dossier médical partagé, systèmes d'information, etc.
- Principaux acteurs
  - Patient, Professionnel de santé et médico-social, Établissements de santé, Hébergeur, ASIP-santé, CNIL, etc.

Module 2 : Droits des patients et secret

- Droits des patients
  - Confidentialité de leurs données de santé, information et accès aux données, droit de rectification et d'opposition, etc.
- Secret
  - Secret professionnel, secret médical, secret partagé

Module 3 : Gestion des données personnelles de santé

- Licéité des traitements de données personnelles
- Recueil des données de santé
- Formalités préalables, PIA
- Élaboration et tenue du registre des activités de traitement
- Conservation, suppression, anonymisation et archivage des données
- Transferts internationaux de données
- Gestion des droits des personnes concernées

Module 4 : Sécurité du système d'information de santé

- Obligations légales de sécurité de données et systèmes d'information de santé
- Enjeux de la sécurité du SI-S : Confidentialité, Intégrité, Disponibilité, Traçabilité et imputabilité
- PGSSI-S

Module 5 : Interopérabilité du système d'information de santé

- Obligation légale d'interopérabilité
- Présentation du cadre d'interopérabilité des systèmes d'information de santé

Module 6 : Hébergement des données de santé

- Exigences légales en matière d'hébergement
- Certification HDS
- Passage de l'agrément à la certification
- Médecin de l'hébergeur de la procédure d'agrément à la certification

Module 7 : SMSI

- Présentation de la norme ISO 27001
- Organisation de la sécurité
  - Rôles et responsabilités, Politique de sécurité, SMSI
  - Médecin hébergeur
  - Responsabilités vis-à-vis du CSP
- Gestion des risques
  - Appréciation des risques
  - Plan de traitement des risques
  - Déclaration d'applicabilité étendue
  - ISO27018
  - Exigences HDS
- Processus de certification
- Mesures de sécurité opérationnelles
  - Gestion des accès, identification, authentification
  - Classification et chiffrement
  - Architecture réseau et applicative
  - Sécurité des échanges
  - Durcissement des systèmes
  - Objets connectés et accès distants
  - Cycle de vie et obsolescence des systèmes
  - Sauvegarde et archivage
  - Auditabilité (Traçabilité, Imputabilité)
- Gestion des incidents dans les contextes des données de santé
  - Notifications aux autorités
- Gestion de la continuité d'activité

Formation « Sécurité du cloud computing »

Réf : SECUCLOUD

Le cloud computing s'est imposé comme un des dernières évolutions majeures de l'informatique et quasiment aucune organisation ni aucun métier ne peut y échapper. Si la gestion des prestataires en général a toujours été un enjeu depuis les premières infogérances, avec le cloud la gestion de la sécurité de ses fournisseurs de cloud vient immédiatement à l'esprit. Les risques sont à la fois techniques, organisationnels et juridiques. Les solutions pour les maîtriser sont en premier lieu juridiques, et cette formation vise à permettre aux consommateurs d'en prendre conscience et de savoir s'en servir.

Objectifs

- Exposer, analyser et hiérarchiser les risques liés au cloud computing
- Proposer des solutions et des bonnes pratiques
- Permettre une maîtrise des clauses contractuelles d'un contrat de cloud

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Toute personne qui est ou envisage de devenir clients de solutions de cloud computing
- DSI, RSSI, chef de projet, responsable opérationnel
- Responsable métier, gestionnaire de contrats, gestionnaire de risque
- Consultant en sécurité et en infonuagique
- Responsable juridique, juriste

Pré-requis

- Cette formation ne nécessite pas de pré-requis particulier.

Méthode pédagogique

- Cours magistral avec de nombreux exemples anonymisés

Supports

- Support de cours au format papier en français
- Tous les documents nécessaires à la formation en français ou anglais
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- Cette formation n'est pas certifiante.

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Programme

Rappels sur le cloud

Rappel sur la cybersécurité

- Risque et gestion des risques
- Menaces et vulnérabilités
- Disponibilité
- Confidentialité
- Gestion des incidents

Risques avec le cloud

- Enfermement
- Perte de gouvernance
- Gestion du projet
- Plan d'Assurance Sécurité
- Suivi de la sécurité

Contractualiser les exigences de sécurité

- Sources du droit
- Généralités sur les contrats
- Preuve

Contenu du contrat de cloud

- Comité de suivi sécurité
- Envoi des données
- Obligations du client
- Prérogatives du prestataire
- Données personnelles et les nouvelles obligations issues du RGPD
- Obligations générales de sécurité
- Confidentialité
- Convention de service attendu
- Développements applicatifs
- Audits de sécurité
- Réversibilité
- Résiliation
- Effacement des données
- Responsabilité contractuelle

Cloud et charte informatique

- La notification d'une violation de données personnelles en vertu du RGPD comment en pratique concilier l'enquête interne avec les délais imposés et la notification d'un incident à l'ANSSI

Comptes à privilèges

Panorama des normes et référentiels

- ISO27001/ISO27002
- SOC1/SOC2
- ISO27017
- ISO27018
- ISO27552

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « Droit de la cybersécurité »

Réf : SECUDROIT

La cybersécurité ne se gère pas qu'avec une organisation adaptée et des savoir-faire techniques, le droit en est un des piliers incontournables, et tout professionnel de la sécurité des systèmes d'information doit en connaître les bases.

Le cours aborde les principaux aspects juridiques de la sécurité informatique, de façon pratique, concrète et pragmatique. La formation est conçue conjointement par des juristes ou avocats et des ingénieurs en informatiques.

Objectifs

- **Apprendre les règles juridiques encadrant la sécurité informatique**
- **Permettre à des personnes n'étant pas juristes de comprendre les règles de droit s'appliquant à la sécurité informatique**
- **Savoir comment assurer le respect du droit de manière efficace et opérationnelle**
- **Pouvoir améliorer le niveau de conformité de son organisme ou de ses clients**

Durée & horaires

- **3 jours soit 21 heures**
- **De 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **RSSI, DSI**
- **Administrateurs systèmes et réseaux, astreintes opérationnelles**
- **Maîtrises d'œuvre de la SSI, chefs de projet, responsables de compte**
- **Consultants en sécurité**
- **Juristes amenés à intervenir dans le domaine de la cybersécurité**
- **Toute personne impliquée dans la sécurité informatique**

Pré-requis

- **Aucun pré-requis n'est demandé. Il n'est pas nécessaire de disposer de connaissances en droit ou en sécurité informatique pour suivre cette formation. Cependant, une connaissance générale de l'informatique est souhaitable.**

Méthode pédagogique

- **Le cours se veut avant tout pratique. Chaque thème est abordé en partant des dispositions juridiques, qui sont expliquées en langage courant. Le formateur conseille les stagiaires sur le comportement qu'il estime le plus pertinent en pratique, en prenant en compte l'ensemble des aspects (coûts, image, risques, etc.).**
- **Le cours est conçu pour être totalement interactif : les stagiaires peuvent constamment poser des questions, et le formateur soumet souvent des cas pratiques aux stagiaires, afin qu'ils réfléchissent au comportement le plus adapté.**

Supports

- **Support de cours au format papier en français**
- **Extraits de documents pratiques : charte informatique, fiches de traitement, etc.**
- **Certificat attestant de la participation à la formation**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUDROIT par HS2.**

Programme

1 - Introduction
- Présentation de la formation
- Présentation du cadre juridique français
- Articulation du droit national avec les droits étrangers

2 - Les atteintes à la sécurité du SI
- Notion essentielle : responsabilité pénale et civile / infractions
- Les infractions d'atteintes au SI
- La collecte des preuves
- Le dépôt de plainte
- Les services spécialisés
- Les obligations de signalement des atteintes au SI

3 - Les obligations de sécurité
- Les obligations légales de sécurité : sécurité des données personnelles, des données de santé, des données bancaires, etc.
- Les obligations contractuelles : disponibilité du service, confidentialité des données, etc.
- Les responsabilités de chacun :
  - de l'organisme
  - de l'employeur
  - des salariés
  - du RSSI, du DSI, de l'administrateur système

4 – La protection des données personnelles
- Le cadre légal : les textes, les principes fondamentaux, les risques associés aux manquements
- Les principales notions : données à caractère personnel, traitement, responsable de traitement, sous-traitant, personnes concernées, DPO, CNIL.
- Les obligations :
  - La cartographie des traitements
  - La conformité des traitements
  - La responsabilité des acteurs : responsable de traitement, co-responsable, sous-traitant, DPO
  - Les études d'impact (PIA)
  - La sécurité des données
  - Les prestataires et sous-traitants
  - Les transferts internationaux
  - Les droits des personnes concernées
- Les contrôles de la CNIL
- Pour aller plus loin : Gouvernance, Code de conduite, Certifications

5 - Les obligations de conservation des traces
- Données relatives au trafic
- Données d'identification des créateurs de contenus
- Accès administratif aux données de connexion
- Autres traces

6 - Surveillance des salariés
- Le pouvoir et devoir de contrôle de l'employeur
- Le respect de la vie privée des salariés
- L'accès au poste et aux données des salariés
- Les règles encadrant l'usage du SI
- La responsabilité du salarié
- La Charte informatique :
  - son rôle
  - son contenu
  - son entrée en vigueur
  - sa valeur contraignante

7 - Conclusion
- Conclusion
- Démarche documentaire
- Outils de veille

Examen

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « ISO 27701 Lead Implementer »

(ex. 27552) – Privacy Information Management System (PIMS)

Réf : ISO27701LI

Avec l'entrée en application du RGPD, les exigences en matière de protection des données personnelles se sont renforcées. Le principe d'accountability est au cœur de la réglementation. Pourtant il n'existe pas encore de certification ni de label permettant aux organismes de démontrer leur conformité au RGPD.
La norme ISO 27701 est une étape importante vers la création d'une certification relative à la protection des données personnelles. Extension des référentiels ISO 27001 et ISO 27002, elle définit un cadre et énumère les mesures nécessaires à la mise en œuvre d'un PIMS (Privacy Information Management System) ou Système de management des données personnelles.
La formation ISO 27701 – Privacy Information Management System (PIMS) d'HS2 est dédiée à cette nouvelle norme. Son objectif est de présenter les apports de l'ISO 27701 aux référentiels ISO 27001 et ISO 27002 afin de permettre aux stagiaires d'implémenter et d'auditer un processus PIMS, notamment dans un contexte RGPD.

Objectifs

- **Présenter le RGPD, les principes et les enjeux de la protection des données personnelles**
- **Présenter l'articulation de la norme ISO 27701 avec les référentiels ISO 27001 et ISO 27002**
- **Présenter les apports de la norme ISO 27701 en matière de protection des données personnelles, notamment dans un contexte RGPD**
- **Présenter les différentes étapes d'implémentation d'un PIMS (Système de management des données personnelles)**
- **Présenter les éléments utiles pour auditer un PIMS**

Durée & horaires

- **5 jours soit 40 heures réparties en 31h30 de cours, 5h00 de travail individuel sur les exercices le soir et 3h30 d'examen.**
- **Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **RSSI**
- **DPO**
- **Responsable conformité**
- **Consultants cybersécurité**
- **Consultants RGPD**

Pré-requis

- **Connaître les normes ISO27001 et ISO27002 est indispensable.**
- **Connaître le RGPD est un véritable plus.**
- **Pour information, la norme ISO 27701 n'existe actuellement qu'en anglais.**

Méthode pédagogique

La méthode pédagogique se base sur les quatre points suivants :

- **Cours magistral basé sur les normes ISO 27701, ISO 27001, ISO 27002 et ISO 29100.**
- **Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.**
- **Exercices pratiques individuels et collectifs effectués par les stagiaires.**
- **Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de certification Certi-Trust ISO 27701 Lead Implementer. A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 3h30 en français. L'examen est constitué d'une partie QCM sur les notions de cours et d'une partie rédactionnelle sous forme d'étude de cas.**

Programme

1 - Introduction : Rappel du cadre général

- 1.1 - Protection des données personnelles et RGPD
- 1.2 - SMSI – Système de management de la sécurité de l'information
- 1.3 – Panorama des normes ISO dédiées à la protection de la vie privée
- 1.4 – Présentation générale de la norme ISO27701

2 – Processus PIMS – Privacy Information Management System

- 2.1 - Présentation des briques du processus PIMS
- 2.2 – Notion de protection des données personnelles (protection of privacy)
- 2.3 – La protection des données personnelles intégrée au système de management
  - -> Intégration de la protection des données personnelles aux différentes briques du processus

3 – Mesures de protection des données personnelles

- 3.1 – Présentation générale des mesures
- 3.2 – Focus sur les mesures clefs de la protection des données personnelles
  - -> Présentation des mesures essentielles de sécurité des données personnelles

4 – Mesures de protection des droits à la vie privée

- 4.1 – Au-delà de la sécurité, la conformité aux autres principes du RGPD
- 4.2 – Conditions de collecte des données
- 4.3 – PIA – Privacy impact assessment
- 4.4. – Droits des personnes concernées
- 4.5 – Concepts de Privacy by design and by default
- 4.6 – Transferts de données
- 4.7 – Sous-traitance

5 – Boîte à outils

-> Documentation du PIMS, Indicateurs, Veille et documents tiers utiles

6 - Focus sur l'audit

- 6.1 – Rappel de la méthodologie d'audit
- 6.2 - Grille d'audit et Documentation

7 – Conclusion

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Nos Intervenants
Formations en vie privée, droit de la cybersécurité

François Coupez dispense les formations :
DPO -CERTIFDPO - RECERTDPO - SECUDROIT

Erik Boucher de Crèvecoeur dispense la formation :
ISO27701LI

Amélie Deleuze dispense la formation :
SECUDROIT

Pierre Desmarais dispense les formations :
SECUSANTE - ISO27701LI

Hadi Elkhoury dispense la formation :
PIA

Olivier Iteanu dispense les formations :
SECUCLOUD

Alexandre Magloire dispense la formation :
SECUSANTE

Elisabeth MANCA dispense la formation :
SECUCOUD

Amélie Paget dispense les formations :
RGPD - DPO - RECERTDPO - ISO27701LI

Géraldine Péronne dispense les formations :
DPO - RGPD

Diane Rambaldini dispense les formations :
DPO - CERTIFDPO - RECERTDPO - PIA

Hervé Schauer dispense la formation :
SECUCLOUD

Clémence Scottez dispense les formations :
DPO -CERTIFDPO - RECERTDPO

Emmanuel Jouffin dispense la formation :
SECUDROIT

HS2
Hervé Schauer Sécurité

Bulletin d'inscription

Merci de retourner ce bulletin soit par courrier à HS2 – 10, rue des Poissonniers – 92200 Neuilly-sur-Seine –
Soit par courriel à formation@hs2.fr

Responsable Formation

Nom et Prénom : .....
Fonction : ..... Société : .....
Adresse : .....
Code postal : ..... Ville : .....
Tél. : ..... E-mail : .....

Souhaite inscrire la ou les personne(s) suivante(s) au(x) stage(s) mentionné(s) :

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

Adresse de facturation (si différente)

Société : ..... Adresse : .....
Code postal : ..... Ville : .....
Nom du correspondant : ..... Tél. : .....
E-mail : .....
N° de TVA intracommunautaire .....

Établissez-vous des bons de commande avec des références à reporter sur notre facture ? oui ❍ non ❍
Si oui, l'inscription sera confirmée uniquement à réception de votre bon de commande.

Demande de subrogation via votre OPCO* : oui ❍ non ❍
*Dans le cas d'une subrogation de paiement via votre OPCO, l'inscription sera confirmée uniquement à réception du contrat ou de l'accord de prise en charge de votre OPCO et de notre convention de formation signée et tamponnée

Date :
Cachet et signature de l'employeur

Convention de formation : pour chacune des sessions proposées, une convention de formation est disponible sur simple demande.
Attention, la prise en compte de votre demande d'inscription sera effective uniquement à réception d'un mail de confirmation par nos services.
Pour tout renseignement complémentaire, vous pouvez contacter le service formation par mail à formation@hs2.fr ou par téléphone au +33 974 774 390.

Retrouvez-nous sur notre site : **www.hs2.fr**

Renseignement / inscription à nos formations, n'hésitez pas à nous contacter :

Lynda Benchikh / Elisa Keller / Estelle Dubois

☎ +33 (0)974 774 390

formation@hs2.fr

Déclaration d'activité enregistrée sous le numéro 11922236092
auprès du préfet de région d'Ile-de-France

Pour nous contacter :

☎ +33 (0)974 774 390 / +33 (0)644 014 072

formation@hs2.fr

Pour nous suivre :

@HS2formation

@HS2formation

@HS2formation

Datadock Organisme Référencé

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'action suivante : **ACTIONS DE FORMATIONS**