

Analyse et pilotage stratégique du projet de mise en conformité de la gestion de données

RS5333 · RS · Publiée

L'essentiel

Code(s) NSF	326, 320, 128
Formacode(s)	13235
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	20/01/2021
Date d'échéance	20/01/2026

Certificateur(s)

INSTITUT D'ETUDES POLITIQUES DE PARIS - SCIENCES PO (IEP) · SIRET : 19753431600017

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification permet de confirmer les compétences acquises en matière de gestion des données personnelles. Elle permet d'accéder à une démarche méthodologique partant de l'analyse des risques encourus dans le périmètre existant jusqu'à la mise en place, le pilotage et le suivi d'un plan de conformité préalablement construit en fonction de la nature, du volume et des finalités des données recueillies. La création et le traitement de données personnelles sont soumis à des obligations destinées à protéger la vie privée et les libertés individuelles. Ainsi acquise, la certification vise à garantir les compétences nécessaires à la protection des données qui pourront ainsi être traitées et pilotées plus efficacement.

COMPÉTENCES ATTESTÉES

- C1. Analyser les responsabilités et les risques liés à l'exercice de la gestion de données en s'appropriant le cadre réglementaire et juridique de la protection des données personnelles pour le placer dans une perspective historique, européenne et internationale, ainsi que politique et sociétale.
- C2. Analyser les spécificités et les champs d'application du Règlement Général de la Protection des Données (RGPD) pour identifier les obligations applicables à une organisation selon son secteur d'activités, la nature de sa structure et son implantation.
- C3. Définir le périmètre d'intervention et les enjeux de la mise en conformité de la gestion des données pour avoir la capacité de l'assumer de manière efficace afin d'apporter une stratégie d'accompagnement pérenne dans la mise en conformité des données personnelles.
- C4. Assurer une veille permanente sur le thème de la protection des données personnelles pour disposer de l'expertise requise sur les plans juridique, technique, opérationnel et sectoriel, dans un cadre national et international.
- C5. Identifier les acteurs, les services et les parties prenantes (internes et externes) traitant les données pour organiser le recueil d'informations auprès des responsables concernés par la gestion des données personnelles de l'organisation
- C6. Recenser les fonctions et les activités de l'organisation nécessitant le traitement de données personnelles pour réaliser l'inventaire des traitements utilisés, depuis la collecte jusqu'à l'archivage.
- C7. Dresser une classification des données personnelles en fonction de leur intérêt, de leur sensibilité, des durées et des modalités de conservation pour évaluer l'existant et établir la cartographie des risques.
- C8. Analyser le niveau de protection et de sécurisation des données pour détecter d'éventuelles non-conformités de leur traitement avec le règlement général des données personnelles.

- C9. Hiérarchiser les risques à partir de la cartographie pour organiser des analyses d'impact (Data Protection Impact Assessment) sur les traitements de données présentant un risque élevé afin de décider de procédures correctives.
- C10. Élaborer un « plan de conformité » en s'appuyant sur des recommandations fonctionnelles, organisationnelles et techniques pour mettre aux normes la gestion des données personnelles d'une organisation.
- C11. Élaborer un « plan d'actions de conformité » de la gestion des données personnelles et calibrer les moyens nécessaires pour planifier et organiser la mise en place des procédures techniques et organisationnelles de sécurisation et de protection des données personnelles répondant aux exigences de la réglementation.
- C12. Concevoir les scénarii de crise, le PCA (plan de continuité d'activité) et le PRA (plan de reprise d'activité) pour mettre en place les mesures adéquates permettant d'assurer la poursuite et la reprise des activités ainsi que l'accès aux données dans des situations critiques.
- C13. Rédiger les mentions légales et adapter les documents contractuels, y compris ceux concernant les prestataires, pour les mettre en correspondance avec les obligations légales.
- C14. Mettre en place les modalités d'accès aux données pour l'exercice des droits sur les données personnelles (droit d'accès, droit de rectification, droit à la portabilité, retrait du consentement, droit d'effacement) imposés par la CNIL (loi Informatique et Libertés) et par le RGPD.
- C15. Alimenter le registre des traitements et organiser la documentation interne sur les traitements des données personnelles et leurs incidents (violation de données) afin de se mettre en conformité avec le RGPD et assurer la traçabilité des événements en cas de contrôle.
- C16. Mettre en place et animer un cadre opérationnel de pilotage et de gouvernance de la conformité pour garantir l'application et la réussite du plan de conformité de l'organisation, à l'aide des techniques et la méthodologie de conduite du changement pour garantir et optimiser la mise en place du « plan de conformité ».
- C17. Élaborer des programmes de formation et de sensibilisation auprès des parties prenantes (internes et externes) pour les fédérer autour des enjeux du « plan de conformité » afin de l'inscrire efficacement et durablement dans la politique de l'organisation.
- C18. Mettre en place des processus de signalement et de notification de violation des données personnelles pour instruire les situations contentieuses et les signalements aux autorités de contrôle afin de limiter les risques de sanctions civiles, pénales et administratives.
- C19. Contrôler, via des audits internes, le respect du « plan de conformité » de gestion des données personnelles afin de mesurer l'efficacité des actions mises en place et les améliorer, le cas échéant.

Secteur d'activité et type d'emploi

RÉGLEMENTATIONS D'ACTIVITÉ

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue

PRÉREQUIS À L'ENTRÉE EN FORMATION

La certification s'adresse à des collaborateurs dont les activités sont en lien avec les données personnelles, de tous métiers : opérationnels, fonctions support et transverses.

Les candidats doivent justifier d'un diplôme de niveau 6 (bac+ 3) ou équivalent et/ou d'une expérience professionnelle de 2 ans de minimum.

COMPOSITION DU JURY — FORMATION CONTINUE

Le jury de certification est composé:

du/de la président.e du jury, extérieur.e à Sciences Po, ayant une expertise particulière en matière de protection des données,

d'un.e membre du jury, extérieur.e à Sciences Po, ayant une expertise particulière en matière de protection des données,

du/de la directeur.rice de la certification au sein de Sciences Po Executive Education.

Base légale

Date de décision	20/01/2021
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	20/01/2026

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.sciencespo.fr/executive-education/certificat-data-protection-officier>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/5333/>

Entrées et sorties de formation

Entrées en formation	3
Parcours menés à terme	2
Taux d'achèvement	67 %
Période	03/2022 – 11/2022

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	5
Montant total engagé	25 400 €
Coût moyen par dossier	5 080 €
Durée moyenne	108 h
Période	10/2021 – 03/2022
Reste à charge titulaire	60 %
France compétences	40 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.