

RGPD DANS L'ASSURANCE

Se mettre en conformité avec le règlement

2 JOURS, 14 HEURES

CONFORMITÉ

CODE : AJU03

Objectifs de la formation

Cerner la réglementation RGPD et ses impacts sur les missions dans l'assurance

Intégrer les exigences en matière de data formulées dans Solvabilité II et les adapter à ses pratiques métier

Déployer une méthodologie pour mettre en place les exigences réglementaires relatives à la gestion des données

Adapter sa relation avec l'ACPR

Animée par

- **BROGLI Marine**
CEO & Data Privacy Expert,
DPO CONSULTING
- **CHEMTOB Sylvain**
Président,
DPO CONSULTING SUD EST
- **OTHMANI Saber**
Juriste IT & Data Privacy Consultant,
DPO CONSULTING

Public concernés

- DPO, responsable conformité, risk manager, correspondant CNIL, directeurs généraux, les services juridiques, les services informatiques

Prérequis

- Cette formation entre dans le champ d'application des dispositions relatives à la formation professionnelle continue car considérée comme une action d'adaptation et de développement des compétences des salariés.

Tarifs

- Promotion estivale - L'Argus de l'assurance Formations : 1435,50 €HT
 - Tarif général : 1595,00 €HT
-

La réglementation RGPD

La nouvelle définition des données personnelles : distinguer données personnelles / non personnelles

- Définition juridique et extrait de la Loi Informatique et Libertés
 - Exemples concrets de données personnelles
-

Le nouveau rôle de délégué à la protection des données : prérogatives renforcées, rôle de conseil et de sensibilisation, point de contact

- Liste des missions du DPO
 - Partage d'expérience et échanges sur les contours de la fonction de DPO
-

Faire le point sur l'« accountability »

- Définition de la notion
 - Etude des spécificités réglementaires propre à l'accountability
-

Les nouveaux droits des personnes : transparence, portabilité, droit à l'oubli, droit à l'opposition au profilage

- Liste des nouveaux droits des personnes
 - Etude des exceptions aux droits des personnes
-

Les responsabilités du sous-traitant

- Liste des obligations du sous-traitant
 - Parallèle avec les responsabilités du responsable de traitement
-

La nouvelle gestion des sous-traitants : grille d'évaluation de la conformité avant sélection, obligations contractuelles, clauses contractuelles types, audits réguliers

- Énonciation de l'article du RGPD
- Etude d'une check-list pour la gestion de la sous-traitance

Assurer la traçabilité des informations et des données (cartographie des transferts) chez les sous-traitants

- Cartographie des transferts
 - Etude d'une cartographie
-

Les nouvelles sanctions encourues et comment les éviter

- Principe de sanction de la CNIL
 - Etude de sanctions pertinentes
-

RGPD et DDA : convergences dans la mise en conformité

Une nécessaire unification de l'information

- Article 20 DDA & IPID
 - Etude des exigences
-

Une négociation impérative entre le principe de minimisation du RGPD et l'obligation de personnalisation de l'offre aux besoins du demandeur de la DDA

- Directive sur la distribution d'assurances Etude comparative entre DDA et RGPD
-

Une gouvernance synergique marquée par la responsabilisation des acteurs et une formalisation de la conformité

- Article 25 du RGPD et de la DDA
 - Etude comparative entre DDA et RGPD
-

Le droit des données dans Solvabilité II

Les exigences en matière de traçabilité : traçabilité des cheminements et des traitements, cartographie des flux, confidentialité et sécurité des flux

- Directive Solvabilité II
 - Etude documentaire sur les outils utilisés pour la traçabilité
-

Les trois critères de qualité de la donnée : exhaustivité, exactitude, pertinence

- Directive Solvabilité II

- Présentation des critères
-

Les avantages de la qualité des données et à l'inverse les risques liés à la non-qualité

- Directive Solvabilité II
 - Réflexion de groupe sur les avantages et les risques
-

Les impacts de la réglementation sur la lutte contre la fraude

Allier les obligations de transparence, droit à l'oubli, droit à l'opposition au profilage, au métier de l'assurance

- Principes du RGPD de transparence, droit à l'oubli, droit à l'opposition au profilage
 - Etude pratique de la mise en application de ces principes à l'assurance
-

Assimiler les particularités des traitements de données d'infractions ou de condamnations

- Définitions des données d'infractions ou de condamnations
 - Etude pratique de leur particularités
-

Détecter des fraudes établies à partir de l'analyse des données

Instauration de la nouvelle réglementation RGPD au sein de votre entreprise : méthodologie et étapes-clés

Le registre des activités de traitement : comment le mettre en place, quelles informations inclure

- Définition du registre des activités de traitement
 - Etude pratique de la mise en place du registre de traitement
-

La « Privacy by design » : au cœur des procédures de l'entreprise et dans la mise en œuvre de chaque nouveau projet

- Définition du principe de Privacy by design
 - Exemples concrets de mise en application
-

Le « Security by default » : mettre en place une procédure visant à tester, analyser et évaluer la sécurité des traitements

- Définition du principe de Security by default
 - Exemples concrets de mise en application
-

Établir une classification des données fondée sur le risque : hiérarchiser les données selon leur degré de criticité, évaluer la sensibilité des données

- Définition de la classification des données
 - Etude de la méthodologie de mise en œuvre
-

Assurer la traçabilité des données et des informations (cartographie des transferts)

- Présentation des outils de traçabilité
 - Etude des contenus clés
-

Développer une cartographie des risques sur les données en propre et identifier les actions de prévention adéquates

- Présentation d'une cartographie des risques
 - Etude de la méthodologie de mise en œuvre
-

Mettre en place une procédure de gestion d'incidents : tenir un registre des violations, procédure de notification, réseau de remontée d'information, suivi des incidents

- Procédure de gestion de violation de données
 - Mise en application concrète au sein de l'entreprise
-

Maîtriser l'implémentation des études d'impacts préalables

- Définition d'une étude d'impact préalable
 - Etude de la méthodologie d'implémentation
-

Savoir établir des procédures pour la gestion des plaintes et des droits des personnes

- Procédure de gestion des plaintes et des droits des personnes
 - Mise en application concrète
-

Prévoir la suppression automatique ou l'archivage des données à l'issue de la durée de conservation

- Principe de durée de conservation
 - Etude pratique des actions à implémenter en fin de durée de conservation
-

Déployer les exigences orientées Solvabilité II dans votre entreprise

Définir une gouvernance (pilotage, principes d'organisation, documentation, dictionnaire des données)

- Contours d'une gouvernance de qualité
 - Mise en application concrète au sein de l'entreprise
-

Formaliser une politique de la qualité des données

- Process d'une politique de la qualité des données
 - Mise en application concrète au sein de l'entreprise
-

Construire un dispositif de contrôle : fixer des objectifs sur la qualité à atteindre, évaluer régulièrement la qualité, vérifier les sources, construire un plan d'amélioration et de correction de la qualité

- Contours d'un dispositif de contrôle
 - Etude de la méthodologie de mise en œuvre
-

Renforcer l'urbanisation du SI : connaître les exigences particulières quant à la gestion et la sécurité des données

- Définition de la notion de l'urbanisation du SI
 - Etude des éléments du chantier à mettre en place
-

L'ACPR : impacts sur les relations

Les nouvelles fonctions de l'ACPR

Maîtriser les sujets « données » concernés par le contrôle de l'ACPR

Comment notifier l'ACPR en cas de violation de données en interne

- Définition de la notification à l'ACPR
 - Etude de la méthodologie de mise en œuvre
-

Les nouvelles exigences de l'ACPR en termes de données : qualité, sécurité, gestion, gouvernance, risques

Gérer les contrôles : prouver de la réalité des dispositifs mis en place et leur efficacité

- Présentation du process de contrôle
 - Etude de la méthodologie de conformité
-

Quiz sous forme de QCM : fixation des notions étudiées

Dates

Classe virtuelle Paris

11-12/10/2021 18-19/11/2021

Modalités pédagogiques, d'évaluation et techniques

■ Modalités pédagogiques:

Pour les formations synchrones-présentiel ou classes virtuelles (formations à distance, en direct), les stages sont limités, dans la mesure du possible, à une douzaine de participants, et cherchent à respecter un équilibre entre théorie et pratique. Chaque fois que cela est possible et pertinent, des études de cas, des mises en pratique ou en situation, des exercices sont proposées aux stagiaires, permettant ainsi de valider les acquis au cours de la formation. Les stagiaires peuvent interagir avec le formateur ou les autres participants tout au long de la formation, y compris sur les classes virtuelles durant lesquelles le formateur, comme en présentiel peut distribuer des documents tout au long de la formation via la plateforme. Un questionnaire préalable dit 'questionnaire pédagogique' est envoyé aux participants pour recueillir leurs besoins et attentes spécifiques. Il est transmis aux intervenant(e)s avant la formation, leur permettant de s'adapter aux publics. Pour les formations en E-learning (formations à distance, asynchrones), le stagiaire peut suivre la formation à son rythme, quand il le souhaite. L'expérience alterne des vidéos de contenu et des activités pédagogiques de type quizz permettant de tester et de valider ses acquis tout au long du parcours. Des fiches mémos reprenant l'essentiel de la formation sont téléchargeables. La présence d'un forum de discussion permet un accompagnement pédagogique personnalisé. Un quizz de validation des acquis clôture chaque parcours. Enfin, le blended-learning est un parcours alternant présentiel, classes virtuelles et/ou e-learning.

■ Modalités d'évaluation:

Toute formation se clôture par une évaluation à chaud de la satisfaction du stagiaire sur le déroulement, l'organisation et

les activités pédagogiques de la formation. Les intervenant(e)s évaluent également la session. La validation des acquis se fait en contrôle continu tout au long des parcours, via les exercices proposés. Sur certaines formations, une validation formelle des acquis peut se faire via un examen ou un QCM en fin de parcours. Une auto-évaluation des acquis pré et post formation est effectuée en ligne afin de permettre à chaque participant de mesurer sa progression à l'issue de la formation. Une évaluation à froid systématique sera effectuée à 6 mois et 12 mois pour s'assurer de l'ancrage des acquis et du transfert de compétences en situation professionnelle, soit par téléphone soit par questionnaire en ligne.

■ Modalités techniques FOAD:

Les parcours sont accessibles depuis un simple lien web, envoyé par E mail aux stagiaires. L'accès au module de E-learning se fait via la plateforme 360Learning. La durée d'accès au module se déclenche à partir de la réception de l'invitation de connexion. L'accès aux classes virtuelles se fait via la plateforme Teams. Le(a) stagiaire reçoit une invitation en amont de la session lui permettant de se connecter via un lien. Pour une bonne utilisation des fonctionnalités multimédia, vous devez disposer d'un poste informatique équipé d'une carte son et d'un dispositif vous permettant d'écouter du son (enceintes ou casque). En ce qui concerne la classe virtuelle, d'un microphone (éventuellement intégré au casque audio ou à la webcam), et éventuellement d'une webcam qui permettra aux autres participants et au formateur de vous voir. En cas de difficulté technique, le(a) stagiaire pourra contacter la hotline au 0170 72 25 81, entre 9h et 17h ou par mail au logistique@infopro-digital.com et la prise en compte de la demande se fera dans les 48h.