

La conformité RGPD, c'est quoi?

Le **Règlement Général sur la Protection des Données** (RGPD ou *GDPR*) est une réglementation globale portant sur la protection des renseignements personnels. Les états membres de l'Union Européenne (UE) ont longtemps garanti des dispositions légales strictes afin de protéger les données à caractère personnel, colligées en ligne par les entreprises et les organisations; le RGPD est un nouveau moyen légal d'unifier et de clarifier ces exigences. La législation s'applique à toute société qui recueille les données des résidents de l'UE, indépendamment de son emplacement. De ce fait, le RGPD a un impact sur les exigences de protection des données à l'échelle mondiale, d'autant plus que de nombreux pays tentent d'atteindre le statut d'adéquation requis pour faciliter les transferts internationaux de données.



Pourquoi la préparation à la conformité RGPD est-elle importante?

Des études démontrent que jusqu'à 20% des entreprises n'ont toujours pas suivi les étapes nécessaires pour se préparer à la conformité RGPD. Le RGPD a créé une exigence urgente pour les entreprises opérant au sein de l'UE, ou commercialisant des biens et/ou des services aux résidents de l'UE, à prendre au sérieux la protection des renseignements personnels. Les organisations doivent prendre des mesures afin de mettre en œuvre les principes de protection requis et éviter les amendes et pénalités pour non-conformité. De plus, le non-respect des exigences du RGPD peut nuire à la réputation de votre entreprise, causer des risques de poursuites judiciaires, d'interventions réglementaires, des pertes financières et des dommages opérationnels.

RECONNU EN TANT QU'INNOVATEUR MAJEUR EN PROTECTION DES DONNÉES



Notre approche unique d'aider les organisations à atteindre la conformité GDPR a été reconnue par l'institution de recherche MarketsandMarkets, mettant en vedette Hitachi Systems Security en tant qu'acteur majeur et innovateur clé dans le domaine de la confidentialité des données dans l'étude 2018 "GDPR Services Market by Solution, Service, Organization Size, and Region – Global Forecast to 2023".

Comment une évaluation de conformité RGPD peut vous aider?

Une évaluation de conformité RGPD est un chemin personnalisé vers la conformité qui vous fournit un modèle de risque et un cadre de gestion de protection des données personnelles. Cette évaluation peut aider les organisations à comprendre leur posture de confidentialité, l'écart entre leur posture et le RGPD, les efforts déjà mis en œuvre et pouvant être réutilisés, les personnes, les processus et les technologies disponibles pour réaliser une telle évaluation ainsi que l'appétit au risque de l'organisation en fonction de son niveau de traitement des et de ses flux de données. Avec une évaluation de conformité RGPD, vous pouvez :

- ▶ Tirer profit de la qualité du compte rendu pour se préparer aux audits et aux certifications
- ▶ Comprendre la portée des exigences du RGPD applicables à votre organisation
- ▶ Identifier les écarts entre les exigences du RGPD et votre position actuelle en termes de protection des renseignements personnels
- ▶ Obtenir un plan sur mesure pour atteindre la conformité, en considérant vos risques contextuels
- ▶ Réduire les responsabilités lors de la remédiation en identifiant et en priorisant les risques

Une approche structurée de gestion de la protection des renseignements personnels

Dans le cadre de son offre de services professionnels, Hitachi Systems Security a développé une approche structurée de gestion de la protection des renseignements personnels, qui vise à mettre en œuvre les mesures techniques et organisationnelles pour développer et maintenir les activités visant à se conformer au RGPD. Basée sur la méthodologie d'Évaluation des Risques d'Entreprise, nous identifions les non-conformités et activités de remédiation et ce, en fonction des risques spécifiques de chaque client. Tel qu'indiqué ci-dessous, l'approche structurée de gestion de la protection des renseignements personnels repose sur trois éléments: **Responsabilité, Éléments de preuve et Propriété** (*ownership*).

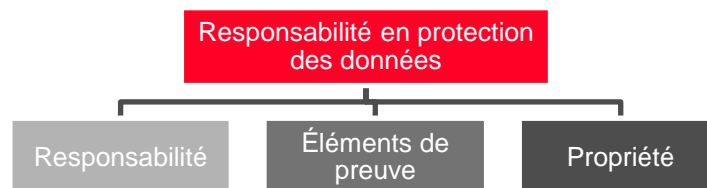


Figure 1: Les éléments de la responsabilité en matière de protection des données personnelles

Éléments d'une évaluation de la conformité au RGPD

Une évaluation de conformité RGPD standard comprend généralement quatre (4) phases distinctes:

✓ Phase 1: Déterminer l'étendue de l'applicabilité

L'étendue de l'applicabilité est essentielle pour examiner le contexte légal et réglementaire spécifiques à votre organisation, établir vos obligations en matière de conformité RGPD et identifier la portée appropriée pour la phase 2, y compris les besoins en ressources et les échéanciers.

✓ Phase 2: Analyse des écarts

L'évaluation des écarts vise à déterminer le niveau de la conformité au RGPD, y compris les ressources disponibles à l'interne, tels que les processus, la technologie et les outils en place. En identifiant les mesures techniques ou organisationnelles déjà présentes ou en cours de déploiement, nos clients seront en mesure d'identifier ce qui peut être réutilisée à des fins de conformité au RGPD.

✓ Phase 3: Évaluation des risques

Lors de l'évaluation des risques, les différents départements de l'organisation seront audités pour déterminer quels sont les processus les plus à risque qui doivent être traités en priorité pour respecter le RGPD et éviter de lourdes amendes en cas de violation des données.

✓ Phase 4: Manuel de gestion et de reddition de comptes

Le manuel personnalisé de gestion et de reddition de comptes en matière de protection des renseignements personnels sert de guide pour les activités continues liées à la conformité. Nous identifions avec vous les domaines qui doivent être traités en priorité, décrivons les contrôles recommandés et répertorions les mécanismes requis pour vous permettre de démontrer la conformité.

VOUS VOULEZ EN APPRENDRE PLUS?

Consultez notre article de blog "[GDPR: Frequently Asked Questions](#)" (en anglais).

