Le cadre de protection de la vie privée du NIST :
Un guide rapide pour les petites et moyennes entreprises

« Le cadre de protection de la vie privée du NIST a été l'un des outils que nous avons pu utiliser, même lorsque nous n'étions pas en mesure de recruter une grande équipe chargée de la protection de la vie privée. »
- Jaime Lees, responsable des données, gouvernement du comté d'Arlington

Qu'est-ce que le cadre de protection de la vie privée du NIST et comment mon organisation peut-elle l'utiliser ?

Le cadre de protection de la vie privée du NIST se veut un outil volontaire qui peut aider votre organisation à créer ou à améliorer un programme de protection de la vie privée. Gérer efficacement les risques liés à la vie privée renforce la confiance, améliore la communication sur vos pratiques et assure la conformité. Une cybersécurité solide est essentielle, mais elle ne suffit pas à éliminer tous les risques pour la vie privée.

Utilisez le cadre de référence pour la protection de la vie privée en suivant les phases « À vos marques, prêt, partez », et alignez votre organisation sur les cinq domaines clés : Identifier, Gouverner, Contrôler, Communiquer et Protéger.

À VOS MARQUES...

Préparez votre programme de protection de la vie privée en utilisant le cadre pour établir une base solide d'identification et de gestion des risques.

Identifier :

- Identifiez les données que vous traitez (collecte, utilisation, partage, stockage) et décrivez leur cheminement dans vos systèmes tout au long du cycle de vie des données - de la collecte à l'élimination. Pas besoin de tout aborder immédiatement, mais c'est un bon début pour avoir une idée plus claire des risques concernant la protection de votre vie privée.
- Utilisez votre carte des données pour évaluer les risques de protection de la vie privée et identifier les problèmes potentiels pour les personnes, tels que l'embarras, la discrimination ou la perte économique. Évaluez ensuite les conséquences pour votre organisation si ces problèmes surviennent (comme la perte de confiance des clients ou l'atteinte à la réputation), ce qui peut avoir un impact négatif sur vos résultats.
- Informez-vous sur les contrats et services utilisés pour votre entreprise afin de garantir qu'ils reflètent vos priorités en matière de protection de la vie privée.

Traduit pour le NIST par TaikaTranslations LLC sous le contrat {133ND23PNB770271}.

Gouverner :

- La culture de la protection de la vie privée commence au sommet de la hiérarchie. Déterminez les valeurs de protection de la vie privée (par exemple, l'autonomie humaine, l'anonymat, la dignité, la transparence, le contrôle des données) sur lesquelles votre organisation se concentre. Alignez vos valeurs et politiques de protection de la vie privée avec l'évaluation des risques pour renforcer la confiance dans vos produits et services.
- Connaître vos obligations légales en matière de protection de la vie privée afin d'élaborer des produits et des services conformes.
- Informez votre personnel sur ses rôles et responsabilités pour qu'il puisse mieux gérer les risques de vie privée lors de la conception et du déploiement des produits et services.
- Réévaluez régulièrement les risques d'atteinte à la vie privée pour voir s'ils ont changé. Cela peut se produire lorsque vous apportez des améliorations à vos produits et services, lorsque vous modifiez votre traitement des données ou lorsque vous prenez connaissance de nouvelles obligations légales.

« Le cadre de protection de la vie privée peut devenir un véritable atout différenciant sur le marché et permettre à l'organisation de développer ses activités.
- *Mary N. Chaney, CISSP, CIPP, directrice de la sécurité de l'information et de la protection de la vie privée, ESPERION Therapeutics, Inc.*

PRÊT...

Avec une compréhension des risques, des obligations légales et une structure de gouvernance en place, l'organisation peut maintenant se concentrer sur les politiques et capacités techniques des systèmes, produits et services.

Contrôler :

- Recueillez-vous, partagez-vous ou conservez-vous des données dont vous n'avez pas besoin ? Réfléchissez à la manière dont vos politiques vous aident, vous ou d'autres organisations, à garder le contrôle des données et sur la façon dont chacun peut également contribuer.
- Tenez compte des risques d'atteinte à la vie privée et des obligations légales lorsque vous décidez de la fonctionnalité de vos systèmes de traitement des données, de vos produits ou de vos services. Envisagez une conception flexible afin de pouvoir répondre de manière plus rentable à l'évolution des préférences des clients en matière de protection de la vie privée et à un environnement juridique dynamique.

- Quels types de traitement de données mettez-vous en œuvre ? Plus vous pouvez dissocier les données des personnes et des appareils, plus les gains en termes de respect de la vie privée sont importants. Considérez comment des mesures techniques comme la dépersonnalisation ou le traitement décentralisé peuvent aider à atteindre vos objectifs tout en protégeant la vie privée.

Communiquer :

- Élaborez des politiques de communication interne et externe sur vos activités de traitement des données.
- Améliorez la transparence en fournissant des avis clairs ou en mettant en place des alertes et signaux pour informer les clients des activités de traitement des données et des choix disponibles.
- Réalisez-vous des enquêtes ou des groupes de discussion afin d'éclairer la conception de vos produits ou services ? Incluez la protection de la vie privée afin d'en savoir plus sur les préférences des clients en matière de protection de la vie privée.
- Anticipez vos actions en cas de violation de données. Comment fournirez-vous des notifications ou des mesures correctives telles que la surveillance ou le gel du crédit ?

Protéger :

- Contrôlez qui se connecte à votre réseau et utilise vos ordinateurs et autres appareils.
- Utilisez des logiciels de sécurité pour protéger les données.
- Cryptez les données sensibles, au repos et en transit.
- Effectuez des sauvegardes régulières des données.
- Mettre régulièrement à jour les logiciels de sécurité, en automatisant ces mises à jour si possible.
- Mettre en place des politiques formelles pour l'élimination en toute sécurité des données et des anciens appareils.

« Si vous devez mettre en place un programme de protection de la vie privée, le cadre de protection de la vie privée du NIST est un point de départ idéal. »
- Jeewon Serrato, associé, BakerHostetler

PARTEZ !

C'est le moment de passer de là où vous êtes aujourd'hui à là où vous voulez vraiment aller.

- Comment votre programme se situe-t-il par rapport à ce que nous avons suggéré ici ?
- Établissez un ordre de priorité parmi les résultats visés et élaborez un plan d'action.

- Discutez de votre plan en tant qu'organisation et utilisez-le pour travailler à l'acquisition des ressources et à la constitution de la main-d'œuvre nécessaires pour atteindre vos objectifs.
- Mettez votre plan en œuvre ! Vous progressez solidement vers un renforcement de la confiance dans vos produits et services, communiquer plus efficacement sur la protection de la vie privée avec vos partenaires et vos clients, et respecter vos obligations en matière de conformité !