Règlement Général sur la Protection des Données (RGPD de l'UE)

Comment la certification BSI ISO/IEC 27001 peut-elle vous aider ?

1 378 509 261 enregistrements divulgués en 2016

58.6% des incidents sont liés à une usurpation d'identité en 2016

3 776 738 documents perdus ou volés en moyenne chaque jour

1 792 incidents de violation de données en 2016

Source: The Breach Level Index

Nous savons que la législation sur la protection de la vie privée telle que le nouveau Règlement Général sur la Protection des Données (RGPD de l'UE) est au cœur de votre programme d'activités. Mais que peut faire votre organisation pour s'y préparer ? Examinez la certification ISO/IEC 27001 avec BSI.

La norme ISO/IEC 27001, internationalement reconnue, vous offre un cadre des meilleures pratiques pour gérer vos risques en matière de sécurité de l'information, y compris ceux liés aux informations personnelles et à la vie privée. La certification vous oblige à démontrer que vous vous conformez aux obligations légales telles que le RGPD de l'UE. De plus, elle favorise une conception responsable et sécurisée, ce qui montre un engagement en faveur de la protection des informations, y compris les données personnelles.

Qu'est-ce que le RGPD de l'UE ?

Le Règlement Général sur la Protection des Données (RGPD) est une nouvelle réglementation autour de la confidentialité des renseignements personnels qui entrera en vigueur à partir du **25 mai 2018**. Il vise à harmoniser les législations protégeant les données dans l'ensemble du marché européen et à permettre aux citoyens de retrouver le contrôle de leurs données personnelles.

Qui cela affecte-t-il ?

- Les contrôleurs et les processeurs de données personnelles
- Tous les États membres de l'UE, ainsi que toute organisation qui opère sur le marché de l'UE et dispose d'informations sur les citoyens européens

Quel est le lien entre ISO/IEC 27001 et le RGPD de l'UE ?

Évaluation du risque

Les amendes élevées qui seront appliquées par la nouvelle réglementation (jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires mondial annuel de la société mère) pourraient avoir un impact financier important sur votre entreprise. La norme ISO/IEC 27001 vous oblige à effectuer une évaluation du risque sur vos actifs d'information qui devrait tenir compte du risque accru pour les informations personnelles et des implications financières potentielles.

Conformité

La nouvelle loi entrera en vigueur le 25 mai 2018, vous devez donc revoir vos obligations. La norme ISO/IEC 27001 impose d'avoir une liste et de respecter des exigences législatives, réglementaires et contractuelles.

Classification des données

Les données à caractère personnel doivent être traitées d'une manière qui assure une sécurité appropriée. La norme ISO/IEC 27001 demande aux entreprises de veiller à ce que les informations bénéficient d'un niveau suffisant de protection en fonction de leur importance.

Déclaration de notification de violation

Les entreprises devront alerter les autorités gérant les données dans les 72 heures suivant la découverte d'une violation de données personnelles.

La norme ISO/IEC 27001 exige qu'un processus de gestion des incidents soit mis en place avec des événements de sécurité de l'information signalés par les canaux de gestion appropriés le plus rapidement possible.

Coopération avec les autorités

Dans le cadre du RGPD de l'UE, les organisations doivent coopérer avec les autorités, par exemple les régulateurs de la protection de la vie privée ou de la protection des données.

La norme ISO/IEC 27001 exige que « les contacts appropriés avec les autorités compétentes soient maintenus ».

Gestion des actifs

Le RGPD de l'UE vous oblige à comprendre les données personnelles que vous collectez, la façon dont vous les obtenez, où elles sont stockées, combien de temps elles sont conservées et qui y a accès. La norme ISO/IEC 27001 vous oblige à identifier les actifs organisationnels et définir les responsabilités de protection appropriés. Vous devez compléter un inventaire des actifs, comprendre qui possède les actifs, quelle est l'utilisation acceptable de ces actifs et la façon dont vous allez les récupérer.

Protection intégrée de la vie privée

L'adoption "Protection intégrée de la vie privée" est une autre exigence du RGPD de l'UE. La norme ISO/IEC 27001 garantit que la sécurité de l'information est conçue et mise en place comme une partie intégrante de l'ensemble du développement et du cycle de vie des systèmes d'informations.

Relations avec les fournisseurs

Le RGPD de l'UE s'applique aux fournisseurs qui traitent des données personnelles pour le compte d'autrui ; il faut que des contrôles et des restrictions soient inclus dans les accords formels. Cela s'applique aux fournisseurs d'accès à internet et aux centres de données externalisés. La norme ISO/IEC 27001 exige la protection des biens de l'entreprise qui sont accessibles par les fournisseurs et pour les organisations, pour surveiller la prestation de services des fournisseurs à l'égard des exigences de sécurité de l'information.

Documentation

En vertu du RGPD de l'UE, les contrôleurs doivent conserver la documentation concernant la vie privée, par exemple les besoins pour lesquels les informations personnelles sont recueillies et traitées, les « catégories » de sujets et les données personnelles. La norme ISO/IEC 27001 exige que la documentation soit conservée en fonction de la complexité des processus et de leurs interactions.

Y-a-t-il autre chose que je dois considérer au-delà de la norme ISO/IEC 27001 ?

La norme ISO/IEC 27001 est un excellent cadre pour démontrer que vous êtes engagé en faveur de la sécurité des informations et de la confidentialité. Elle prend en charge bon nombre des exigences du RGPD, mais vous devriez également considérer :

- **Formation et sensisbilisation**
  Assurez-vous que vos chefs d'entreprise et les principaux intervenants soient conscients de cette modification de la loi. Si vous voulez vous sentir plus informé, nous avons une gamme de cours sur la protection des données que vous voudrez peut-être considérer, comme notre formation aux fondements du Règlement Général sur la Protection des Données.
- **Désigner un Data Protection Officer (DPO)**
  Certaines activités, comme le suivi à grande échelle des personnes physiques ou le traitement de données de catégories spéciales, exigent que l'organisation nomme un délégué à la protection des données. Même si vous n'en avez pas nécessairement besoin, il est recommandé de nommer un délégué à la protection des données avec une connaissance de la sécurité des informations et une compréhension de la loi sur la protection des données.
- **Donnez un coup d'œil aux procédures**
  Assurez-vous d'avoir des procédures qui couvrent tous les droits des personnes. Cela inclut la façon dont vous vous assurez que les informations personnelles sont exactes, utilisées aux fins de la collecte et conservées uniquement pour la durée nécessaire, et de la manière dont vous fournissez ou supprimez des données personnelles.
- **Améliorez votre système**
  Si vous traitez ou stockez des informations dans le cloud public, la norme ISO/IEC 27018 peut également vous aider. Elle s'appuie sur un système de l'ISO/IEC 27001 et s'assure que vous mettez des exigences spécifiques en place pour protéger les renseignements personnels identifiables.

  Vous voulez encore plus de conseils ?
  BS 10012 est le cadre des meilleures pratiques pour un système de gestion des informations personnelles. Il a récemment été mis à jour afin de mieux s'aligner aux exigences de l'UE en matière de RGPD.

Pourquoi BSI ?

Nous avons été à l'avant-garde des normes de sécurité protégeant les informations depuis 1995, après avoir produit la première norme BS 7799, devenue la norme ISO/IEC 27001. Et nous ne nous sommes pas arrêtés là, abordant des problèmes émergents tels que la sécurité cybernétique et le cloud. C'est pourquoi nous sommes le mieux placés pour vous aider à gérer la confidentialité et à vous conformer à la réglementation.

bsi.

Pour en savoir plus
Appelez au : **+33 (0)1 55 34 11 40**
Visitez : **bsigroup.com/cyber-fr**