bsi.

...making excellence a habit.™

EU Règlement Général sur la Protection des Données (RGPD)

20 étapes vers la conformité au RGPD

- Une approche méthodique, systématique et logique

Livre blanc

Résumé du rapport

Le Règlement Général sur la Protection des Données (RGPD) a remplacé la directive 95/46/CE sur la protection des données en mai 2018. Bien que de nombreuses entreprises aient déjà aligné leurs processus et procédures sur la directive, le RGPD impose aux entreprises un certain nombre de nouvelles exigences qui ne s'appliquaient pas dans le passé. Au vu de l'augmentation des amendes pour non-respect du RGPD pouvant atteindre jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires global mondial, le prix à payer pour la non-conformité peut être conséquent pour votre entreprise. Ce livre blanc décrit 20 mesures pratiques que vous pouvez prendre pour vous assurer que votre entreprise peut adopter une position défendable et mettre en œuvre et maintenir un programme de conformité au RGPD efficace.

Contexte

Nécessité d'une réforme de la protection des données de l'UE

Malheureusement, la directive de 1995 sur la protection des données a été interprétée différemment dans les pays de l'UE, de sorte que le régime d'application peut varier considérablement d'un pays à l'autre et, dans certains cas, même à l'intérieur du même pays.

Beaucoup de choses ont changé depuis 1995 : les téléphones mobiles et les tablettes sont omniprésents et l'utilisation d'un téléphone mobile ou l'accès à Internet à partir de n'importe quel appareil laisse une trace numérique qui peut être reliée à un individu. L'essor des médias sociaux et la prolifération des applications qui suivent chaque détail de notre vie numérique laissent à penser qu'une réforme complète de la réglementation en matière de protection des données n'a jamais été aussi importante.

Les objectifs de la réforme

La réforme de la réglementation en matière de protection des données comprend cinq objectifs fondamentaux que l'on peut résumer comme suit :

- Renforcer les droits des individus (la vie privée dès la conception et par défaut)
- Renforcer le marché intérieur de l'UE par de nouvelles règles claires et solides pour la libre circulation des données
- Assurer l'application cohérente des règles
- Définir des normes globales de protection des données
- Assurer un niveau élevé de protection des données dans tous les secteurs d'activité

Téléphone : +33 (0)1 55 34 11 40 E-mail : contact.france@bsigroup.com Consulter : bsigroup.fr

Les règles se transforment en principes

Pour atteindre les objectifs susmentionnés, les huit règles actuelles de protection des données évoluent pour devenir un ensemble de principes et de droits d'accès de la personne concernée. Cependant, bien qu'il semble s'agir d'un changement important, l'intention fondamentale des exigences demeure la même ; il s'agit en réalité d'un changement structurel ou cosmétique.

Le tableau suivant montre comment les règles et les principes sont liés les uns aux autres :

1. Obtenir et traiter l'information de façon équitable
2. Conserver les données uniquement à une ou plusieurs fins spécifiées et légales
3. Traiter les données uniquement conformément aux fins pour lesquelles elles vous ont été fournies initialement
4. Stocker les données en toute sécurité
5. Conserver des données exactes et à jour
6. S'assurer que les données sont appropriées, pertinentes et non excessives
7. Ne pas conserver les données plus longtemps que nécessaire aux fins précisées
8. Procurer une copie de ses données personnelles à chaque individu, sur demande

→

1. Légalité, équité et transparence
2. Fins limitées
3. Minimisation des données
4. Exactitude
5. Limitations de stockage
6. Intégrité et confidentialité

→

Rec.59; Art.12(2)

- Les contrôleurs ont **l'obligation légale de faire respecter les droits des personnes concernées**

À un niveau élevé, les nouveaux principes et droits imposés par le RGPD peuvent en effet se résumer en trois « principes sous-jacents » de haut niveau : Transparence, Clarté et Responsabilité.

- **Transparence :** faire preuve d'une transparence totale sur les activités entreprises en terme de traitement des données. Il ne doit rien arriver aux données dont les personnes concernées n'ont pas pleinement connaissance.
- **Clarté :** être clair sur ce que sont ces activités de traitement des données. Il n'est plus acceptable d'obscurcir les détails relatifs au traitement des données en utilisant un « jargon juridique » ou une terminologie complexe. Les informations sur le traitement des données doivent être présentées dans un langage clair et compréhensible.
- **Responsabilité :** il faut clarifier, tant au sein des structures organisationnelles qu'envers les personnes concernées elles-mêmes, qui est responsable de la supervision et de la gestion de leurs données ainsi que de l'application des droits des personnes concernées.

20 étapes vers la conformité au RGPD - Approche de BSI

Une approche séquentielle et hiérarchisée - BSI suggère de suivre les étapes suivantes de manière séquentielle, de l'étape 1 à 20 ; dans de nombreux cas, les résultats des premières étapes serviront pour les étapes ultérieures. Par exemple, les flux d'informations et les registres d'informations.

Regroupement des étapes

BSI regroupe les 20 étapes en quatre catégories complémentaires, comme suit :

- **Gouvernance** (6 étapes)
- **Technique** (4 étapes)
- **Opérations** (6 étapes)
- **Communication** (4 étapes)

Considérations avant de commencer

Avant de réaliser les 20 étapes suivantes, BSI a fait l'hypothèse que vous comprenez la place que prend votre entreprise au sein de l'écosystème du RGPD. Assurez-vous que votre entreprise comprend clairement si vous êtes un responsable du traitement des données, un contrôleur de données ou les deux à la fois.

Ensuite, il peut également être utile d'examiner à l'avance les structures de gouvernance existantes au sein de votre entreprise. On pourrait peut-être les utiliser et en tirer parti pour rationaliser davantage le processus de mise en conformité au RGPD.

De même, nous supposons qu'il existe déjà un certain degré de gouvernance (c.-à-d. l'établissement d'un cadre de gestion du risque pour maintenir l'assurance continue de l'efficacité des efforts de conformité, des cadres pour la gestion des modifications, des cadres pour la gestion des projets, etc.). Ainsi, ces étapes sont conçues pour s'intégrer aux structures existantes ; par exemple, les résultats des étapes proposées pour l'évaluation d'impact sur la vie privée (étapes 13 et 14 ci-dessous) pourraient être intégrés aux Comités de Gestion des Risques existants, où le DPO aurait désormais un siège.

Téléphone : +33 (0)1 55 34 11 40 E-mail : contact.france@bsigroup.com Consulter : bsigroup.fr

Etapes de gouvernance

Etape 1 :

Data Protection Officer (DPO)

La première étape consiste à nommer un DPO. En fait, la plupart des entreprises devront déterminer officiellement si elles ont l'obligation de nommer un DPO en fonction du traitement qu'elles entreprennent. Indépendamment du fait que le rôle officiel soit nécessaire ou non, la responsabilité de la protection des données et de la vie privée doit être officiellement attribuée à une personne. Par exemple, un grand cabinet d'avocats n'a pas nécessairement besoin d'un « DPO », mais aura quand même besoin de nommer une personne responsable de la protection des données.

Ceci peut se faire par le biais de :

- L'attribution du rôle de DPO à un salarié existant
- L'embauche d'une personne pour un nouveau poste défini
- L'externalisation du rôle de DPO à un fournisseur DPO Tiers

Indépendamment de la façon dont cette exigence est satisfaite, les entreprises sont tenues aux deux obligations suivantes

- Veiller à ce que le DPO réponde à toutes les exigences en matière de formation et de compétences
- S'assurer que le DPO désigné n'a pas d'autres conflits d'intérêts opérationnels

Pour certaines entreprises, il sera difficile de répondre à ces exigences en raison de la pénurie de compétences dans ce domaine, ce qui entraînera des exigences salariales élevées pour ceux qui possèdent à la fois des certifications et l'expérience en tant que DPO. De même, le coût de l'externalisation du rôle de DPO sera probablement plus élevé au cours des 18 prochains mois.
Répondre au manque de compétences par la formation d'un membre du personnel existant peut également s'avérer coûteux en raison du risque de recevoir de mauvais conseils d'un DPO inexpérimenté, ainsi que du coût d'opportunité de ce membre du personnel qui, dans de nombreux cas, n'est plus en mesure de poursuivre ses activités quotidiennes si un conflit d'intérêts opérationnel est jugé exister.

Etape 2 :

Responsabilité

La responsabilité doit maintenant être clairement attribuée et démontrée pour toutes les activités de traitement des données au sein d'une entreprise.

La meilleure façon d'y parvenir est d'attribuer la responsabilité de la propriété des données aux managers des business unit des secteurs d'activité où les données sont traitées.

Heureusement, la plupart des entreprises comprennent déjà qui est responsable au sein de chaque business unit, au moins sur une base informelle. L'aspect clé de cette étape consistera à s'assurer que la responsabilité et l'obligation de rendre compte sont encrées dans les rôles des propriétaires de données. On peut y parvenir en confiant aux propriétaires des données la responsabilité de remplir les registres de données/d'informations et de compléter les diagrammes de flux de données et d'informations (voir l'étape 3 et l'étape 4).

Etape 3 :

Registre de données/d'informations

La chose la plus importante à retenir au début d'un programme de protection des données est que « vous ne pouvez pas protéger ce que vous ne comprenez pas ». C'est le début du processus de compréhension de vos données. Un format et une structure de registre de données devraient être convenus et toutes les données personnelles que l'entreprise détient ou traite devraient être enregistrées dans ce registre.

Le registre des données (ou des informations) devrait détailler au moins ceci :

- Les noms des systèmes qui contiennent les données personnelles
- Comment les données sont classées
- La finalité du traitement des données
- La base juridique du traitement des données
- La durée de conservation des données
- Les champs spécifiques ou les types de données contenus
- Le propriétaire des données
- La mention du partage des données avec des tiers et l'identification de ces tiers

Conformément à l'étape 2, cette étape doit être accomplie par le propriétaire des données et examinée par le DPO.

Etape 4 :

Diagrammes de flux de données

Dans le cadre des efforts de votre entreprise pour s'assurer que vous évitez les pièges du type « vous ne pouvez pas protéger ce que vous ne comprenez pas », il est important de s'assurer que les acteurs au sein de l'entreprise peuvent comprendre clairement, rapidement et de manière concise leurs activités de traitement des données. Les registres de données créés à l'étape 3 seront d'une utilité limitée à cette fin.
Une représentation schématique est généralement le meilleur moyen de parvenir à une compréhension directe.
Pour chaque activité de traitement des données ou business unit, un diagramme montrant le flux d'informations entrant et sortant de l'entreprise doit être créé.

Les diagrammes doivent inclure :

- Les détails sur les données du client
- Le moyen de réception des données et où elles sont réceptionnées
- Le lieu de stockage
- Le lieu où elles sont transférées en interne
- Le nom des systèmes où elles se trouvent
- Les détails sur les tiers auxquels les données peuvent être transférées (y compris les mesures de sécurité telles que le cryptage)
- Le moyen d'éliminer des données et la fréquence de cette élimination

Conformément aux étapes 2 et 3, cette étape doit être accomplie par le propriétaire des données et examinée par le DPO.

Un autre avantage réel et tangible de ces diagrammes est de pouvoir déterminer rapidement où se trouvent les données. Cela devrait faciliter une réponse efficace aux demandes d'accès des personnes concernées et aux requêtes relatives au droit à l'oubli (voir les étapes 9 et 10).

Etape 5 :

Données pertinentes et non excessives

Maintenant que vous comprenez les données dont vous disposez, vous pouvez considérer la pertinence des informations et l'étendue des informations que vous avez collectées.

Examinez toutes les données dans les registres d'informations/flux de données. En pratique, cela signifie qu'il faut examiner toutes les données et vous poser les questions suivantes : « Avons-nous réellement besoin de ces données ? » et « Avons-nous obtenu ces données et les utilisons-nous équitablement ? »

Si les données ne sont pas absolument nécessaires, supprimez-les et arrêtez de les collecter. Moins vous conservez de données, plus l'effort requis pour maintenir la conformité sur une base continue est faible.

Etape 6 :

Fournisseurs et responsables du traitement des données tiers

Lorsque les données sont partagées avec des tiers, assurez-vous que des accords de sécurité et de confidentialité sont convenus et appliqués par contrat.

Idéalement, les contrats comprendront des clauses contractuelles pour s'assurer que les tiers traitent les données en toute sécurité, conformément aux règlements sur la protection de la vie privée, et vous permettent d'effectuer des vérifications et des contrôles ponctuels afin d'assurer la conformité.

Il devient également pratique courante pour les contrôleurs d'exiger certaines preuves : le responsable du traitement des données est certifié ou respecte au moins une norme de sécurité des informations comme la norme ISO/IEC 27001.

Téléphone : +33 (0)1 55 34 11 40 E-mail : contact.france@bsigroup.com Consulter : bsigroup.fr

Etapes techniques

Etape 7 :

Gestion du consentement

Dans la mesure du possible, la base juridique sur laquelle vous traitez les données ne devrait pas s'appuyer uniquement sur le consentement. Cependant, BSI reconnaît que ce n'est pas toujours possible.

Ainsi, lorsque le consentement est utilisé comme base pour le traitement des données personnelles, il y aura un certain nombre d'exigences pour assurer la conformité :

- Assurez-vous que le consentement actuellement détenu satisfera aux exigences du RGPD ; si ce n'est pas le cas, obtenez un nouveau consentement.
- Assurez-vous que tous les consentements peuvent être immédiatement démontrés ; dans le cas contraire, obtenez de nouveau le consentement et tenez un registre des consentements.
- En cas de données sensibles (c.-à-d. des données médicales, des données sur la santé, des données sur les demandes d'assurance, etc.), assurez-vous d'obtenir un consentement explicite supplémentaire
- Veillez à ce que le processus de retrait du consentement soit clairement communiqué à tous les points où des données sont collectées et dans un cadre de confidentialité.
- Identifiez toutes les données relatives aux moins de 18 ans ; assurez-vous que le consentement d'un tuteur a été fourni, sinon, obtenez un nouveau consentement.

Etape 8 :

Conservation des données

Après avoir fait le point sur les actions clés des étapes précédentes, les raisons du traitement des données et la durée de conservation des données sont maintenant assimilées. Le processus d'application de cette période de conservation peut maintenant commencer.

Examinez vos registres de données et diagrammes de flux de données et, là où les données ont dépassé les délais de conservation convenus, vous devez maintenant les supprimer en toute sécurité.

Etape 9 :

Droit des personnes concernées

Un certain nombre des droits des personnes concernées ont été clarifiés ou introduits. Cela exigera à la fois des approches techniques et de gouvernance pour mettre en place des processus d'intervention conformes.

D'abord du point de vue de la gouvernance, les entreprises doivent s'accorder sur la politique et les processus de gouvernance pour répondre à ces exigences et les documenter.

- Demandes d'accès par la personne concernée
- Droit à la restriction du traitement/objection
- Droit de rectification
- Droit à l'oubli
- Droit de ne pas être soumis à la prise de décision automatisée / droit de ne pas faire l'objet de profilage
- Portabilité des données

Etape 10 :

Droits des personnes concernées (étape technique)

Deuxièmement, d'un point de vue technique, les entreprises doivent se mettre d'accord sur leur approche technique pour répondre aux exigences clarifiées et récentes concernant les invocations des droits des personnes concernées. Elles sont également tenues de documenter cette approche.

- Demandes d'accès par la personne concernée
- Droit à la restriction du traitement/objection
- Droit de rectification
- Droit à l'oubli
- Droit de ne pas être soumis à la prise de décision automatisée / droit de ne pas faire l'objet de profilage
- Portabilité des données

Etapes opérationnelles

Etape 11 :

Réponses aux violations de données

Le RGPD introduit une nouvelle obligation de signalement des violations, en vertu de laquelle les violations doivent être signalées à l'autorité de surveillance compétente (et également aux personnes concernées) dans les 72 heures. Cette période de 72 heures s'avérera difficile à respecter dans le meilleur des cas ; sans un processus de réponse bien compris et régulièrement mis à l'essai, les entreprises seront presque certainement en deçà de cette obligation.

Les entreprises doivent se mettre d'accord sur leur processus d'intervention en cas de violation des données ou d'incident de sécurité des données et documenter ce processus. Ce système doit être mis à l'essai périodiquement pour s'assurer qu'il demeure adapté à l'usage prévu en cas de violation des données en situation réelle. La mise en place d'un exercice de simulation de violation des données permettra d'identifier les lacunes dans le processus et de s'assurer que l'entreprise est prête à intervenir efficacement en cas de violation de données.

Etape 12 :

Réponses aux violations de données

Après avoir tiré des leçons et compris certaines choses lors des étapes précédentes, les données traitées et les parties avec lesquelles les données sont partagées sont maintenant comprises.

Examinez vos registres de données et vos diagrammes de flux, ainsi que les lieux où les données sont reçues, partagées ou transférées. Revoyez également les dispositions de sécurité en place. En cas de problème de sécurité potentiel, signalez-le pour examen et mesure corrective. Idéalement, cela peut être fait en conjonction avec votre service de sécurité de l'information en interne ou avec vos consultants externes en sécurité.

Ceci doit être fait pour tous les ensembles de données et tous les diagrammes de flux de données produits (soit à la fois les données au repos et les données en transit).

Etape 13 :

Evaluation d'impact sur la vie privée (EIVP) préliminaire

L'une des nouvelles exigences du RGPD est l'idée de mettre en œuvre le « respect de la vie privée dès la conception et par défaut » ; ce qui était historiquement la meilleure pratique est désormais devenu une exigence légale à respecter.

Pour mettre ce principe en pratique, les entreprises sont désormais tenues d'effectuer des évaluations d'impact sur la vie privée (EIVP).

Une EIVP est un processus d'examen des activités de traitement des données du point de vue du risque. En réalité, il s'agit d'une évaluation des risques propres à la nature du risque d'atteinte à la vie privée des personnes concernées par le traitement des données.

Pour cette étape, BSI suggère d'effectuer une évaluation préliminaire d'impact sur la vie privée ; toutes les données actuellement stockées ou traitées doivent être examinées afin de s'assurer que tout risque potentiel en matière de protection de la vie privée est identifié et que les préoccupations sont présentées à la direction pour examen.

Pour être précis, la réalisation d'une évaluation préliminaire d'impact sur la vie privée rétroactive n'est PAS une exigence légale spécifique dans le cadre du RGPD.

MAIS...

Dans le cas d'une violation de données ou d'une plainte pour non-conformité retenue par une autorité de surveillance, si la vulnérabilité ou la lacune du processus a été découverte dans le cas d'une évaluation d'impact sur la vie privée rétroactive, l'amende pour un tel événement serait beaucoup plus élevée. À cet égard, la réalisation d'une EIVP préliminaire pourrait être considérée comme une police d'assurance contre un tel événement.

Téléphone : +33 (0)1 55 34 11 40 E-mail : contact.france@bsigroup.com Consulter : bsigroup.fr

Etape 14 :

Évaluation d'impact sur la vie privée (EIVP) opérationnelle

Une partie des nouvelles exigences du RGPD relative à la mise en œuvre du « respect de la vie privée dès la conception ou par défaut » est que les évaluations d'impact sur la vie privée doivent être effectuées dans les deux circonstances suivantes :

- Nouvelle collecte ou nouveau traitement de données personnelles
- Nouvelle utilisation ou nouvelles fins introduites pour des données personnelles déjà en possession d'une entreprise

Les entreprises doivent se mettre d'accord sur une approche cohérente, systématique et reproductible pour les évaluations d'impact sur la vie privée en continu lorsque les circonstances susmentionnées se produisent. Cette approche doit être documentée.

D'après l'expérience de BSI, le meilleur moyen d'y parvenir est d'intégrer des passerelles ou des déclencheurs à travers d'autres processus préexistants, à savoir :

- Le cycle de vie des développements logiciels (SDLC)
- La gestion de projets
- La gestion des modifications
- L'approvisionnement, etc.

Ainsi, par exemple, du point de vue de la gestion des modifications, nous suggérons qu'une question passerelle soit ajoutée au formulaire de demande de modification : « Cette modification génèrera-t-elle une nouvelle collecte de données personnelles ou une nouvelle utilisation des données personnelles existantes ? », Si la réponse est oui, cela invoquera un processus d'EIVP.

Etape 14 :

Engagement de la direction

La supervision de la gestion des activités de traitement des données a toujours été la meilleure pratique ; dans le cadre du RGPD, il s'agira désormais d'une obligation légale. Les personnes qui siègent à la direction ou au conseil d'administration devront désormais faire preuve d'engagement et de compréhension du traitement des données au sein de leur entreprise

Pour ce faire, le DPO doit disposer de temps pour présenter le profil actuel de protection des données de l'entreprise en tant que sujet permanent lors des réunions du conseil d'administration.

Afin de s'engager correctement avec les membres de la direction et de leur transmettre ce dont ils ont désormais besoin, les informations pertinentes et les indicateurs de performance clés devront être convenus et présentés à la direction et au conseil d'administration.

BSI suggère que les KPI comprennent au moins les éléments suivants :

- Incidents
- Manquements évités de justesse
- Demandes d'accès
- Risques d'entrave à la vie privée à surveiller/résultats des EIVP
- Données partagées avec des tiers et plans de surveillance de la conformité

Etape 16 :

Tenue des dossiers de traitement de données détaillés

Conformément à l'article 30 du RGPD, les entreprises sont à présent dans l'obligation légale de tenir des registres détaillés des opérations de traitement des données.

En vertu de nos premières étapes où des registres de données et des diagrammes de flux de données ont été produits, les entreprises qui appliquent notre ensemble d'étapes suggérées respecteront déjà les principes fondamentaux de cette exigence. Cependant, des dossiers supplémentaires doivent également être tenus à jour.

BSI suggère que les dossiers comptent au moins ce qui suit :

- Registre des informations
- Registre des données conservées
- Registre des transferts au tiers
- Registre des demandes d'accès par la personne concernée
- Registre des droits à l'oubli
- Registre des plaintes
- Registre des tiers, etc.

Etapes de communication

Etape 17 :

Formation

Comprendre l'importance de la protection des données a toujours été essentiel pour les entreprises. C'est toujours le cas aujourd'hui. Dans le cadre du RGPD, il est désormais obligatoire de s'assurer que les employés reçoivent une formation appropriée à leur rôle au sein de l'entreprise.

Dans la pratique, cela signifie que tous les membres du personnel doivent recevoir une formation sur les pratiques de protection des données au sein de l'entreprise, à la fois lors de leur intégration et au moins une fois par an. De plus, si le personnel traite des données personnelles dans le cadre de ses fonctions quotidiennes, on s'attendra à ce qu'il reçoive une formation appropriée sur les pratiques adéquates et sécuritaires de traitement des données. Cela nécessitera souvent une formation adaptée aux emplois qu'ils exercent.

Etape 18 :

Politique de protection des données

D'un point de vue interne, l'entreprise doit redéfinir sa politique actuelle de protection des données pour tenir compte des résultats de tous les processus susmentionnés.

La politique devra mettre l'accent sur la façon dont elle respecte les principes du RGPD et fournir des conseils au personnel sur les pratiques appropriées en matière de protection des données.

En outre, BSI suggère que, pour répondre aux obligations de transparence et de clarté, la politique de protection des données des entreprises doit également servir de notice de confidentialité interne ; la politique doit clairement répondre au besoin de traitement des données du personnel dans le cadre de leur emploi (c'est-à-dire quelles données personnelles du personnel sont stockées ou traitées, et pour quelles raisons, combien de temps elles seront conservées, comment invoquer les droits de la personne concernée, etc.).

Etape 19 :

Avis de confidentialité

D'un point de vue externe, l'entreprise doit redéfinir son avis de confidentialité pour tenir compte des résultats de tous les processus susmentionnés.

La notice de confidentialité doit expliquer clairement aux clients ou aux autres tiers dont vous stockez les informations quelle est exactement la nature du traitement des données effectué.
Pour satisfaire aux obligations de transparence, la notice de confidentialité des entreprises doit être disponible (ou au moins mentionné) à chaque point où les données sont recueillies. La notice doit être claire pour tous les intervenants externes :

- Les données dont nous disposons
- Pourquoi nous les détenons
- Ce que nous en faisons
- C'est ici que nous les stockons
- Nous les conservons pour cette durée
- Voici la manière dont vous pouvez exercer vos droits
- Voici ceux avec qui nous les partageons
- Voici la personne à contacter si vous avez une question sur la protection de la vie privée

Etape 20 :

Communication

Publiez et diffusez la politique de protection des données et la notice de confidentialité mises à jour à tous les intervenants concernés (internes et externes).

Toutes les personnes concernées (internes et externes) peuvent désormais être considérées comme informées des pratiques de l'entreprise en matière de protection des données et conscientes de la manière d'invoquer les droits de la personne concernée.

Il convient de noter que ce degré de transparence doit se traduire par un engagement accru de la part des personnes concernées ; davantage de demandes d'accès ou de droit à l'oubli seront probablement reçues, ce qui augmentera la une charge administrative des entreprises. C'est en grande partie ce qu'implique le RGPD. Cependant, en supposant que toutes les étapes précédentes suggérées dans ce livre blanc ont été accomplies, les entreprises n'ont rien à craindre ; les processus réactifs devraient être résilients et toute perturbation potentielle devrait être réduite au minimum.

Téléphone : +33 (0)1 55 34 11 40 E-mail : contact.france@bsigroup.com Consulter : bsigroup.fr

Marché cible

Ce livre blanc concerne et sera utile à tous ceux qui participent au traitement, au stockage et à la gestion des informations personnelles. Il s'agit des personnes suivantes :

- Les DPO récemment nommés
- Les gestionnaires des ressources humaines
- Les directeurs des ventes et du marketing
- Les professionnels de la sécurité de l'information
- Les responsables de la conformité et de l'audit
- Les professionnels de la santé
- Les propriétaires de petites entreprises où des données personnelles sont traitées
- Les équipes de dirigeants qui cherchent à comprendre la voie vers la conformité

Conclusion

Nous comprenons la valeur des données pour votre entreprise et les conséquences graves d'une violation de données. Nous aidons les entreprises à appliquer les meilleures pratiques de gestion et de maintien de la conformité aux normes de protection des données de l'UE, tout en conservant la capacité d'utiliser les données au profit de l'entreprise.

Nous préconisons fortement une approche fondée sur le risque pour aider à promouvoir l'utilisation responsable des données. En suivant les 20 étapes ci-dessus, les entreprises peuvent se positionner conformément aux exigences du RGPD.

Cyber sécurité et résilience de l'information

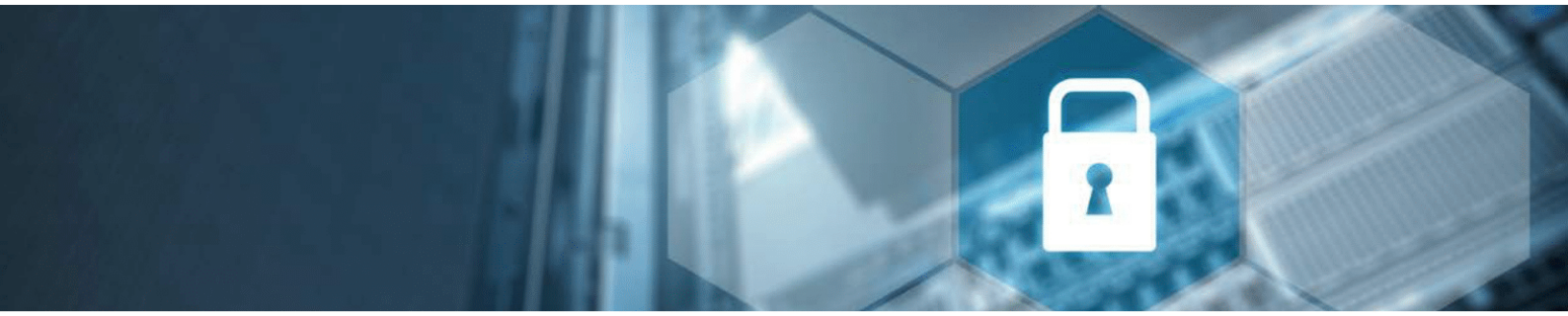
L'approche « Cybersécurité et résilience de l'information » de BSI vous aide à relever vos défis en matière d'information. Nous permettons aux entreprises de sécuriser les informations, les données et l'infrastructure critique contre les menaces changeantes qui affectent votre personnel, vos processus et vos systèmes tout en renforçant la gouvernance de l'information et en assurant la résilience.

Chez BSI, nous créons de l'excellence chez nos clients à travers la mise en place de normes. Nous permettons aux organisations de mieux fonctionner, de gérer leurs risques et de parvenir à atteindre une croissance durable. Depuis plus d'un siècle, nos experts refusent les notions de médiocrité et complaisance pour aider les entreprises à intégrer l'excellence aussi bien dans leur façon de travailler que dans les produits qu'elles créent.

Nous faisons de l'excellence une habitude.

BSI permet aux organisations d'améliorer leur business en se servant des normes comme pratiques d'excellence. Depuis plus d'un siècle, BSI a soutenu les meilleures pratiques et œuvre à les mettre en place dans des organisations du monde entier. Avec plus de 86 000 clients répartis dans 193 pays, BSI est une entreprise véritablement internationale dont les compétences couvrent de nombreux secteurs, comme l'automobile, l'aérospatial, la construction, l'alimentaire et la santé. Avec son expertise dans le développement de normes, les services d'assurance et services professionnels, BSI améliore la performance commerciale et aide ses clients à se développer de manière durable, à atténuer les risques et à devenir plus résilients.

Pour en savoir plus, consultez **bsigroup.fr**



bsi.

En savoir plus

Téléphone : **+33 (0)1 55 34 11 40**

Site internet : **www.bsigroup.fr**

BSI/UK/xxxx/CIR/1117/EN/BLD