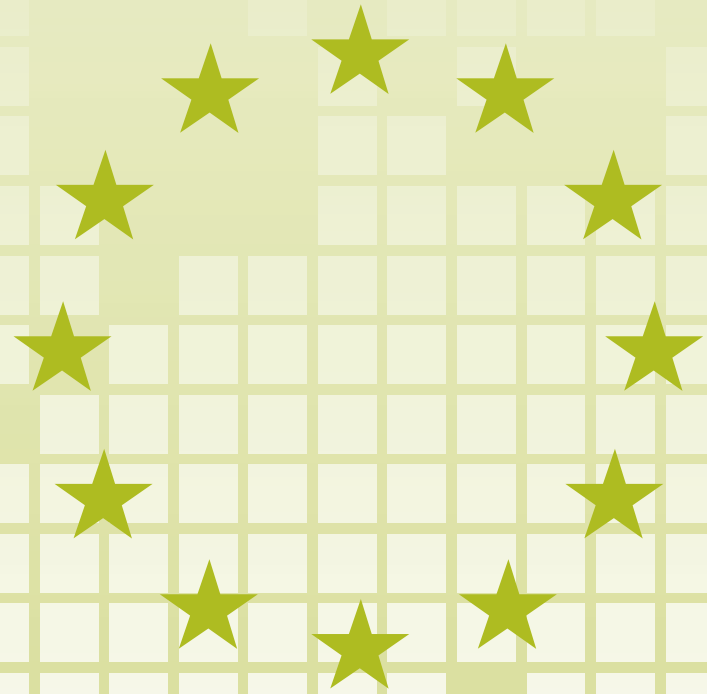
RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

PRÉPAREZ-VOUS EN 13 ÉTAPES



CPVP
Commission de la protection de la vie privée

PRÉPAREZ-VOUS EN 13 ÉTAPES

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

1. CONSCIENTISATION

Informez les personnes clés et les décideurs quant aux changements à venir. Ils doivent évaluer les conséquences que le RGPD aura sur l'entreprise ou l'organisation.

2. REGISTRE DE DONNÉES

Faites l'inventaire des données à caractère personnel que vous conservez, notez quelle est leur origine et les personnes avec lesquelles vous les avez partagées. Enregistrez vos traitements. Vous devez éventuellement organiser un audit d'information à cet effet.

3. COMMUNICATION

Évaluez votre déclaration de confidentialité existante et prévoyez les modifications nécessaires à y apporter à la lumière du RGPD.

4. DROITS DE LA PERSONNE CONCERNÉE

Vérifiez si les procédures actuelles dans votre entreprise ou organisation prévoient tous les droits que la personne concernée peut invoquer, y compris la manière dont les données à caractère personnel peuvent être supprimées ou dont les données seront communiquées par voie électronique.

5. DEMANDE D'ACCÈS

Mettez à jour vos procédures d'accès existantes et réfléchissez à la manière dont vous traiterez désormais les demandes d'accès eu égard aux nouveaux délais du RGPD.

6. FONDEMENT LÉGAL POUR LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Documentez les différents types de traitements de données que vous effectuez et identifiez le fondement légal pour chacun d'entre eux.

7. CONSENTEMENT

Évaluez la manière dont vous demandez, obtenez et enregistrez le consentement et apportez les modifications nécessaires.

8. ENFANTS

Développez des systèmes qui vérifient l'âge de la personne concernée et qui demandent le consentement au(x) parent(s) ou au(x) tuteur(s) pour le traitement de données de mineurs.

9. FUITES DE DONNÉES

Prévoyez des procédures adéquates pour détecter, rapporter et analyser des fuites de données à caractère personnel.

10. LA PROTECTION DES DONNÉES DÈS LA CONCEPTION ET L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Familiarisez-vous avec les notions de "protection des données dès la conception" et d' "analyse d'impact relative à la protection des données" et examinez la manière dont vous pouvez mettre en œuvre ces concepts dans le fonctionnement de votre entreprise ou organisation.

11. DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Désignez au besoin un délégué à la protection des données ou une personne qui est responsable du respect des règles de protection des données. Évaluez la place que cette personne occupe au sein de la structure et de la politique de votre entreprise ou organisation.

12. AU NIVEAU INTERNATIONAL

Déterminez de quelle autorité de contrôle vous relevez si votre entreprise ou organisation est active au niveau international.

13. CONTRATS EXISTANTS

Évaluez vos contrats existants, principalement avec des sous-traitants, et apportez les changements nécessaires en temps utile.

INTRODUCTION

LE RÈGLEMENT GÉNÉRAL RELATIF À LA PROTECTION DES DONNÉES (RGPD) EST ENTRÉ EN VIGUEUR LE 24 MAI 2016. LES ENTREPRISES ET ORGANISATIONS ONT TOUTEFOIS JUSQU'AU 25 MAI 2018 POUR SE CONFORMER À LA NOUVELLE RÉGLEMENTATION. PRÉPAREZ-VOUS EN 13 ÉTAPES !

Le RGPD n'est bien entendu pas entièrement nouveau ! Bon nombre de ses concepts et principes fondamentaux sont déjà présents dans l'actuelle loi vie privée belge. Donc celui qui respecte déjà aujourd'hui la législation actuelle pourra prendre cette approche comme point de départ valable pour la mise en œuvre du RGPD. Mais il y a quand même quelques nouveautés et améliorations sensibles qui changeront quelque peu l'approche actuelle.

Grâce à ce manuel et aux informations complémentaires sur le site Internet de la Commission vie privée, vous pouvez repérer les différences entre l'actuelle loi vie privée et le nouveau RGPD et adapter votre politique en fonction. Au cours des prochains mois, la Commission vie privée développera, en collaboration avec les secteurs concernés, des directives et instruments supplémentaires afin de guider les entreprises et organisations dans cette préparation. Au niveau européen, le Groupe article 29 de protection des données se chargera d'apporter l'assistance nécessaire.

Il importe de prendre dès à présent des dispositions afin de faciliter la transition vers la nouvelle réglementation. Assurez-vous pour ce faire du soutien et de la collaboration des personnes clés dans votre organisation. Vous devez ainsi par exemple prévoir de nouvelles procédures pour répondre aux exigences de transparence ou pour garantir les droits de la personne concernée. Dans une grande entreprise ou une structure complexe, cela peut entraîner des conséquences importantes au niveau du budget, de l'informatique, du personnel, de la politique et de la communication.

Le RGPD insiste davantage sur l'obligation de documentation du responsable du traitement, comme preuve de sa responsabilité. Ce manuel aide les entreprises et organisations à évaluer leur politique actuelle en matière de protection des données et à l'adapter aux nouvelles exigences du RGPD. Une première étape dans ce cadre peut consister en la révision des actuels contrats et règlements relatifs à l'échange de données.

Sachez que certaines dispositions du RGPD auront un impact plus important sur votre entreprise ou organisation que d'autres, comme par exemple les dispositions en matière de profilage ou les règles spécifiques de protection des données à caractère personnel des enfants. Il peut donc se révéler utile de dresser d'ores et déjà l'inventaire des dispositions du RGPD qui auront le plus d'impact sur votre entreprise ou organisation et de les mettre en œuvre en premier lieu.

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

CONSCIENTISATION

Veillez à ce que les personnes clés et les décideurs de votre entreprise ou organisation soient informé(e)s de la nouvelle réglementation. Ils doivent en évaluer les conséquences et désigner les domaines qui peuvent aujourd'hui être problématiques à la lumière du RGPD. Si votre entreprise ou organisation dispose d'un registre des risques, il peut constituer un excellent point de départ.
La mise en œuvre du RGPD peut avoir une influence considérable sur les moyens disponibles, surtout en ce qui concerne les entreprises ou structures de plus grande taille ou plus complexes. Utilisez donc en priorité la période de transition de deux ans pour informer les collaborateurs des changements à venir. Ne le reportez pas jusqu'à la dernière minute.

REGISTRE DE DONNÉES

Faites l'inventaire minutieux des données à caractère personnel que vous conservez, notez quelle est leur provenance et les personnes avec lesquelles vous les avez partagées. Il serait intéressant d'enregistrer tous vos traitements. Vous devez éventuellement organiser un audit d'information à cet effet. Ceci s'applique éventuellement à toute l'entreprise ou uniquement à certaines sections déterminées.
Le RGPD introduit quelques nouveaux droits, destinés spécifiquement au monde des réseaux. Lorsque votre entreprise conserve par exemple des données à caractère personnel inexactes et les a partagées avec d'autres organisations, vous devrez informer ces dernières de l'inexactitude afin qu'elles puissent apporter les corrections dans leur propre registre.
Cette obligation de documentation contribue en outre au respect de l'exigence de responsabilité contenue dans le RGPD. Selon ce principe, une entreprise ou une organisation doit prouver qu'elle agit conformément aux principes de protection des données.

COMMUNICATION

Évaluez votre déclaration de confidentialité existante et prévoyez les modifications nécessaires à y apporter à la lumière du RGPD.
Si votre entreprise ou organisation traite déjà des données à caractère personnel, vous devez fournir certaines informations aux personnes concernées, comme l'identité du sous-traitant et la manière dont il utilisera les données. Ces informations sont généralement communiquées sous la forme d'une déclaration de confidentialité.
Le RGPD requiert que cette déclaration de confidentialité soit complétée par de nouveaux types d'information. Il faudra ainsi désormais communiquer le fondement légal du traitement de données et les délais pendant lesquels vous conserverez les informations, préciser si vous échangez les données en dehors de l'Union européenne et prévoir la possibilité pour la personne concernée de porter plainte auprès de la Commission vie privée si elle estime que ses données à caractère personnel sont traitées à tort.
Le RGPD requiert que ces informations soient communiquées de manière concise, dans une langue compréhensible et claire.

DROITS DE LA PERSONNE CONCERNÉE

Vous devez vérifier si les procédures actuelles dans votre entreprise ou organisation prévoient tous les droits que la personne concernée peut invoquer, y compris la manière dont les données à caractère personnel peuvent être supprimées ou dont les données seront communiquées par voie électronique.
Le RGPD prévoit notamment les droits suivants pour la personne concernée :

- ***information et accès aux données à caractère personnel***
- ***rectification et suppression des données***
- ***objection à l'encontre de pratiques de marketing direct***
- ***objection à l'encontre de prises de décision automatisées et de profilage***
- ***portabilité des données***

De manière plus générale, le RGPD offre à la personne concernée les mêmes droits que l'actuelle loi vie privée belge, moyennant quelques améliorations considérables. Si votre entreprise ou organisation est déjà suffisamment équipée pour prévoir ces droits individuels, la transition vers le RGPD se fera relativement facilement. Le moment est bien choisi pour évaluer vos procédures existantes et pour vérifier la manière dont vous procéderez lorsque quelqu'un voudra exercer son droit. Qui prendra la décision ? Les systèmes sont-ils conçus pour y répondre ?
Le droit de portabilité des données est une nouveauté. Il s'agit d'une forme améliorée de l'accès où la personne concernée a le droit d'obtenir les données à caractère personnel la concernant dans un format structuré, couramment utilisé et lisible électroniquement. La plupart des entreprises et organisations le font déjà, mais si vous utilisez encore des impressions papier ou une forme électronique inhabituelle, c'est de nouveau le bon moment pour revoir votre copie.

DEMANDE D'ACCÈS

Prévoyez une mise à jour de vos procédures d'accès existantes et réfléchissez à la manière dont vous traiterez désormais les demandes d'accès eu égard aux nouveaux délais du RGPD.
Le RGPD prévoit de nouvelles règles qui déterminent la manière d'agir à l'égard de demandes d'accès. Dans la plupart des cas, il faudra donner suite à la demande d'accès dans les 30 jours (contre 45 jours actuellement), et ce gratuitement. Des demandes manifestement non fondées ou excessives peuvent être facturées ou refusées. Si votre entreprise ou organisation veut être en mesure de refuser des demandes d'accès, vous devez adapter la politique et les procédures en conséquence.
Vous devez donner à la personne concernée qui demande l'accès certaines informations complémentaires comme les délais de conservation des informations et le droit de faire rectifier des données inexactes. Si votre entreprise ou organisation traite un grand nombre de demandes d'accès, les modifications prévues par le RGPD auront un impact considérable. Il faut qu'au niveau logistique, toutes les demandes puissent être traitées dans le délai prévu et que la personne concernée reçoive les informations nécessaires. Une réflexion approfondie doit être menée à ce sujet.
À terme, il peut se révéler rentable de développer un système grâce auquel la personne concernée peut consulter elle-même les données en ligne. Les entreprises et organisations sont encouragées à réaliser une analyse coûts/bénéfices d'un tel système d'accès en ligne.

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

FONDEMENT LÉGAL POUR LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

6

Documentez les différents types de traitements de données que vous effectuez et identifiez le fondement légal pour chacun d'entre eux.
De nombreuses entreprises et organisations n'ont peut-être pas défini à l'époque un fondement légal pour les traitements de données qu'elles réalisent. En vertu de la législation actuelle, les conséquences pratiques sont peu nombreuses voire inexistantes. Le RGPD change toutefois la donne car les droits de la personne concernée peuvent différer selon la base légale du traitement de données. L'exemple le plus parlant est le fait que la personne concernée dispose d'un droit renforcé pour demander la suppression de ses données si son consentement était à la base du traitement.
Il est important de préciser dans la déclaration de confidentialité le fondement légal qui a été choisi pour le traitement de données et d'indiquer également ce fondement chaque fois que l'on répond à une demande d'accès. Les fondements légaux du RGPD sont quasiment identiques à ceux de l'actuelle loi vie privée. Vérifiez donc quels traitements de données vous effectuez, déterminez la base légale et documentez vos démarches avec soin, à la lumière de l'exigence de responsabilité.

CONSENTEMENT

valuez la manière dont vous demandez, obtenez et enregistrez le consentement et apportez les modifications nécessaires.
Le RGPD mentionne les termes "consentement" et "consentement explicite". La distinction n'est pas très claire, étant donné que le consentement doit dans les deux cas être libre, spécifique, éclairé et univoque. Le consentement doit également se révéler par une manifestation active de l'accord. En d'autres termes, le consentement ne peut pas être déduit tacitement ou à partir d'une case cochée préalablement ou d'une absence d'action. Si vous comptez sur le consentement de la personne concernée pour traiter ses données, veillez surtout à ce que ce consentement réponde aux exigences du RGPD. Si ce n'est pas encore le cas, modifiez votre mécanisme de consentement ou cherchez une alternative au consentement pour justifier le traitement de données. Notez que le consentement doit être contrôlable et que la personne concernée a généralement davantage de droits lorsque vous comptez sur le consentement comme fondement du traitement de données. Le RGPD précise que le responsable du traitement doit être en mesure de démontrer que le consentement a été donné. Évaluez donc les systèmes actuels qui enregistrent le consentement, afin d'assurer une piste d'audit efficace.

7

8

ENFANTS

Commencez dès aujourd'hui à développer des systèmes qui vérifient l'âge de la personne concernée et qui demandent le consentement au(x) parent(s) ou au(x) tuteur(s) pour le traitement de données de mineurs.
Pour la première fois, le RGPD offrira une protection spéciale aux données à caractère personnel d'enfants, en particulier dans le contexte de services commerciaux par Internet tels que les réseaux sociaux. En bref, si votre entreprise ou organisation collecte des données d'enfants – âgés de moins de 16 ans –, un parent ou un tuteur devra donner son consentement pour que le traitement de données soit licite. Cela peut entraîner des conséquences considérables si l'objet de votre entreprise ou organisation est de proposer des services à des enfants et, en tant que telle, collecte leurs données à caractère personnel. Retenez que le consentement doit être contrôlable et que le cas échéant, la déclaration de confidentialité doit être rédigée en des termes compréhensibles pour les enfants.

FUITES DE DONNÉES

9

Prévoyez des procédures adéquates pour détecter, rapporter et analyser des fuites de données à caractère personnel. Évaluez pour ce faire les différents types de données à caractère personnel que vous conservez et documentez celles qui relèveraient de l'obligation de déclaration si une fuite de données survenait. Dans certains cas, vous devez informer directement la personne concernée faisant l'objet de la fuite de données, par exemple lorsque la fuite peut donner lieu à des pertes financières personnelles. Les plus grandes entreprises ou organisations devront élaborer une politique et des procédures pour gérer les fuites de données – soit au niveau central, soit au niveau local. Toutes les fuites de données ne devront pas être signalées à la Commission vie privée – seules celles pour lesquelles il est probable que la personne concernée subira une quelconque forme de dommages, par exemple suite à un vol d'identité ou à la violation d'une obligation de secret. Notez que le non-respect de l'obligation de déclaration peut donner lieu à une amende, outre l'amende pour la fuite de données elle-même.

LA PROTECTION DES DONNÉES DÈS LA CONCEPTION ET L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

10

Familiarisez-vous d'ores et déjà avec les notions de "protection des données dès la conception" et d' "analyse d'impact relative à la protection des données", mieux connues sous les termes suivants : "Privacy by design" et "Privacy impact assessment". Examinez la manière dont vous pouvez mettre en œuvre ces concepts dans le fonctionnement de votre entreprise ou organisation. Ils peuvent être liés à d'autres processus organisationnels tels que la gestion des risques et la gestion des projets. Évaluez d'ores et déjà les situations où il sera nécessaire de réaliser de telles analyses. Qui s'en chargera ? Qui doit y être associé ? L'analyse se fera-t-elle de manière centrale ou de manière locale ?
Intégrer dès le début la protection des données et, dans ce cadre, réaliser une analyse d'impact font partie des "bonnes pratiques" d'une entreprise ou organisation. Il ne s'agissait auparavant que d'une exigence implicite des principes de protection des données. Le RGPD en fait une exigence légale claire.
À noter que vous ne devez pas systématiquement réaliser une analyse d'impact. Celle-ci n'est requise que dans des situations à haut risque, par exemple lorsqu'une nouvelle technologie est mise en œuvre ou lorsqu'une opération de profilage peut entraîner des effets considérables pour les personnes concernées. Lorsque le PIA indique que le traitement de données comporte un "risque élevé", il est nécessaire d'obtenir l'avis de la Commission vie privée quant à la licéité du traitement à la lumière du RGPD.

DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Désignez au besoin un délégué à la protection des données ou une personne qui est responsable du respect des règles de protection des données. Évaluez la place que cette personne occupe au sein de la structure et de la politique de votre entreprise ou organisation. Le RGPD requiert pour certaines entreprises et organisations qu'elles désignent un délégué à la protection des données, par exemple pour les autorités publiques ou les sous-traitants dont la tâche consiste à observer régulièrement et systématiquement des personnes concernées, ce à grande échelle. Il est important que soit une personne de l'organisation, soit un conseiller externe soit responsable du respect des principes de protection des données et qu'une personne ait les connaissances, l'implication et la compétence de le faire. Vous devez dès lors juger dès à présent si votre entreprise ou organisation a l'obligation de désigner un tel délégué. Dans l'affirmative, évaluez si l'approche actuelle correspond aux exigences du RGPD.

AU NIVEAU INTERNATIONAL

Si votre entreprise ou organisation est active au niveau international, vous devez déterminer de quelle autorité de contrôle vous relevez.
Le RGPD prévoit un règlement quelque peu complexe pour déterminer quelle autorité de contrôle prend la direction des opérations lors de l'examen d'une plainte à caractère international, par exemple lorsqu'un traitement de données se rapporte à des résidents de plusieurs États membres. L'autorité chef de file est déterminée selon l'endroit où l'entreprise ou l'organisation a son établissement principal ou selon l'établissement où sont prises les décisions relatives aux traitements de données. Pour un siège principal traditionnel, on peut le déterminer assez facilement. Cela se complique dans le cas d'entreprises ou d'organisations complexes, implantées sur plusieurs sites, où les décisions relatives à différentes activités de traitement sont prises à divers endroits.
Pour savoir clairement quelle autorité de contrôle est en charge de votre entreprise ou organisation, il est conseillé d'établir à quel endroit votre organisation prend ses décisions les plus importantes quant aux traitements de données. Cela vous permettra de déterminer votre "établissement principal" et donc aussi l'autorité de contrôle compétente.

CONTRATS EXISTANTS

Évaluez vos contrats existants, principalement avec des sous-traitants, et apportez les changements nécessaires en temps utile. Le RGPD crée un système intelligent qui établit le rapport entre le responsable du traitement et les sous-traitants. Il détermine même les conditions qui s'appliquent aux activités de sous-traitance. Pour approfondir ces conditions, vous devez évaluer les contrats existants et apporter les modifications nécessaires.
Le RGPD souligne l'importance des mesures de sécurité applicables aux banques de données. En cas d'outsourcing, il est également important d'évaluer si les mesures de sécurité qui étaient prévues dans les contrats existants sont toujours adéquates et répondent aux exigences du RGPD.

VOUS TROUVEREZ PLUS D'INFORMATIONS SUR LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES DANS LE DOSSIER THÉMATIQUE SUR LE SITE INTERNET DE LA COMMISSION VIE PRIVÉE (FR)

Commission de la protection de la vie privée

Rue de la Presse 35 | B-1000 Bruxelles | T+32 (0)2 274 48 00
E-mail: commission@privacycommission.be
Site Internet: http://www.privacycommission.be

Éditeur responsable
W. Debeuckelaere
Impression
Imprimerie centrale de la Chambre des représentants
Design
Design is Dead

Il existe aussi une version néerlandaise de ce manuel.
Er bestaat ook een Nederlandse versie van deze handleiding.
Vous pouvez consulter ou télécharger cette brochure sur le site Internet de la Commission