cirb.brussels
IT is for you

Règlement Général sur la Protection des Données (GDPR)

Guide pratique à l'attention des institutions locales et régionales de la Région de Bruxelles-Capitale

Tables des matières

Avant-propos

Depuis 30 ans, le Centre d'Informatique pour la Région Bruxelloise a pour rôle d'organiser, promouvoir et disséminer l'usage des TIC auprès des autorités et administrations locales de la Région de Bruxelles-Capitale.

Le Centre poursuit à cet effet une **mission d'information**, notamment par des publications faisant le point sur ses activités, ses projets ou l'évolution des technologies.

C'est encore le cas avec cette brochure consacrée au GDPR, le nouveau règlement européen sur la protection des données. L'offre abondante de services en ligne et la multiplication des flux de données personnelles posent avec plus d'acuité encore la problématique de la protection de la vie privée.

L'Union Européenne a donc élaboré ce règlement qui sera d'application le 25 mai 2018.

Cette brochure vous invite à faire le point sur les divers aspects du GDPR. Certains peuvent s'avérer coûteux en argent et/ou en temps que vous, vos collaborateurs et toute votre institution devront y consacrer.

Pour vous assister dans ce travail, le CIRB a développé des services spécifiques (voir page 14) et, ainsi, vous conformer aux prescrits du GDPR.

Bonne lecture !

Hervé FEUILLIEN
Directeur général

Robert HERZEELE
Directeur général adjoint

Nouveau cadre juridique

Le Règlement Général sur la Protection des Données (GDPR en anglais) est une législation européenne qui remplace celle de 1995 et va bien plus loin que la loi belge de 1992 sur la protection de la vie privée actuellement en vigueur[1].

Aujourd'hui, les données sont massivement récoltées et utilisées, notamment dans le cadre de l'économie digitale, de l'e-governement, des médias sociaux, etc. L'Union européenne a souhaité uniformiser les règles existantes pour favoriser l'émergence de ces services tout en protégeant le citoyen de manière équivalente sur tout le territoire européen.

Le GDPR introduit des règles plus sévères, de nouveaux devoirs dans le chef des gestionnaires de données et des sanctions plus lourdes en cas de non-respect.

Il sera d'application le 25 mai 2018.

1 Directive européenne 95/46/CE du Parlement européen et du Conseil du 24/10/1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (J.O.U.E. 23/11/1995).
Loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (MB 18/3/1993).

Testez vos connaissances

	VRAI	FAUX	JE NE SAIS PAS
1. Je suis responsable d'une administration publique, le GDPR ne me concerne pas mais vise uniquement les entreprises privées de plus de 250 employés	○	○	○
2. Le GDPR ne concerne que les données électroniques et pas les documents papier	○	○	○
3. J'ai encore le temps de me mettre à jour, le GDPR n'entrera en vigueur qu'après transposition dans la loi belge en 2020	○	○	○
4. En tant que service public, je suis obligé de désigner un Data Protection Officer (délégué à la protection des données)	○	○	○
5. Mon administration ne gère pas de données sensibles, comme des dossiers médicaux, je ne dois donc pas me conformer au nouveau règlement GDPR	○	○	○
6. Je conserve sur mon ordinateur les coordonnées des personnes qui ont souscrit à ma newsletter. Ces personnes sont donc d'accord de recevoir des mails de ma part. Je suis dès lors en ordre vis-à-vis du GDPR	○	○	○

Vous avez au moins trois VRAI et/ou trois JE NE SAIS PAS ?

Alors prenez le temps de parcourir cette brochure et de vous familiariser avec le nouveau règlement. De nombreux aspects vous concernent. D'autant que vous devez désormais démontrer que vous avez tout mis en œuvre pour sécuriser les données à caractère personnel que vous traitez.

Vous avez au moins trois FAUX ?

Il semble que vous ayez déjà quelques notions sur le nouveau cadre légal induit par le GDPR. Parcourez malgré tout ce document pour vous en assurer. Le CIRB peut vous accompagner dans la mise en conformité de votre institution.

Réponse aux questions : 1 Faux / 2 Faux / 3 Faux / 4 Vrai / 5 Faux / 6 Faux

GDPR, c'est quoi ?

GDPR, c'est l'abréviation anglaise du Règlement Général relatif à la Protection des Données[2].

C'est un règlement européen qui fixe un **nouveau cadre pour la protection et l'échange de données à caractère personnel**. Il sera d'application de manière identique, le même jour, dans tous les pays membres de l'Union européenne.

PRINCIPE

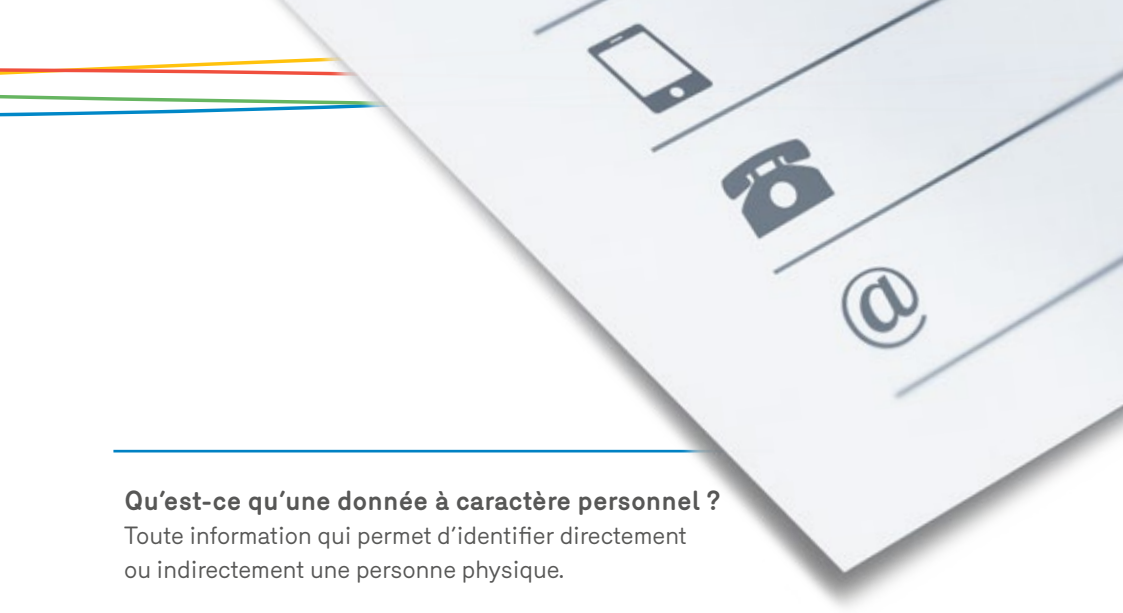
La base du GDPR est la protection des citoyens et la transparence sur ce qui est fait avec leurs données personnelles. La nouveauté réside dans le concept d'**accountability**, c'est-à-dire la responsabilisation des organisations qui traitent de telles données.

Elles doivent **informer et obtenir le consentement** des personnes lorsqu'elles récoltent des données les concernant[3].

- **Informer via une 'Charte vie privée'** qui explique, dans un langage clair et compréhensible, quels types de données sont récoltées, à quelles fins, combien de temps elles seront conservées et à qui elles seront éventuellement transmises.

- Le GDPR maintient le **consentement préalable** du citoyen, mais ajoute la notion de consentement **éclairé et univoque.** Il vous faut aussi conserver la preuve de ce consentement car, en cas de plainte, vous devrez prouver à l'autorité de contrôle que vous l'avez obtenu.
  Fini donc de se partager des fichiers entre collègues pour envoyer une newsletter ou des invitations à un vernissage.

2 General Data Protection Regulation (GDPR). En français, RGPD.
3 Il y a de nombreuses exceptions à ce principe pour le secteur public. Par exemple, le SPF Finances ne doit pas avoir le consentement des personnes pour récolter des données fiscales visant à établir l'impôt des personnes physiques. Ceci fait partie intégrante de sa mission et est soutenu par un cadre juridique spécifique.



Qu'est-ce qu'une donnée à caractère personnel ?
Toute information qui permet d'identifier directement ou indirectement une personne physique.

PAR EXEMPLE : nom, prénom, adresse, numéro de téléphone, numéro de compte en banque ou de carte de crédit, numéro de Registre national, adresse IP, plaque d'immatriculation, dossier médical, login et mot de passe, etc.

SÉCURISER LES DONNÉES

Une fois que vous avez collecté des données à caractère personnel, vous devez également **protéger** ces données au maximum pour éviter, par exemple, **des fuites ou des vols**.

Ici aussi, en cas de problème ou de plainte, c'est à votre organisation qu'il reviendra de prouver qu'elle a mis en œuvre toutes les mesures techniques et organisationnelles requises (y compris la gestion des accès et la protection des données dès la conception d'un produit ou service)[4].

4 Lire plus loin dans le chapitre « Les conséquences du GDPR pour votre organisation » en page 10.

Suis-je concerné·e ?

Une seule réponse : oui !

Vous êtes concerné·e si l'un de vos services, ou un sous-traitant, traite, gère, utilise et/ou dispose de données à caractère personnel[5].

Et c'est plus fréquent qu'on ne le pense. Quelques exemples ?

- Le fichier des lecteurs de la bibliothèque communale
- La liste des abonnés au centre culturel
- Les enfants inscrits dans les crèches communales ou aux activités extra-scolaires
- Les dossiers de patients d'une maison médicale ou d'un home
- Les données conservées électroniquement ou sur papier par les Ressources Humaines
- La liste des personnes à qui vous envoyez une newsletter électronique ou papier
- Les coordonnées de candidats à un logement social, à une allocation de remplacement
- Les données fiscales de demandeurs de primes à l'embellissement des façades ou à l'installation de panneaux solaires
- Un fichier tableur avec des données extraites d'IRISbox[6] ou de BOS[7]
- Toutes les demandes de citoyen en vertu d'une réglementation (permis d'urbanisme, passeport…)
- Etc…

Dès l'instant où vous récoltez – ou traitez – des données personnelles, vous devez vous conformer à un certain nombre d'obligations. Certaines existaient déjà dans la loi belge de 1992 ; le GDPR en instaure de nouvelles (voir page 10).

5 Pour le GDPR, le traitement de données est toute opération ou ensemble d'opérations, automatisées ou non, appliquées à des données, telles que la collecte, l'enregistrement, le conservation, la consultation, la communication par transmission, la diffusion…

6 IRISbox est le guichet électronique de la Région de Bruxelles-Capitale.

7 BOS est l'outil de gestion électronique de toute réunion ou assemblée (gouvernement bruxellois, conseil communal, CPAS…) développé par le CIRB.

Date de mise en œuvre

Le GDPR entre en vigueur le **25 mai 2018** sur l'ensemble du territoire de l'Union européenne.
Pas de dérogation, pas de délai !

C'est un Règlement européen et non une Directive. C'est-à-dire qu'il va s'appliquer de manière uniforme à **tous les pays membres de l'Union européenne, à la même date**, sans exception, sans transposition dans le droit national.

De cette façon, les citoyens européens bénéficient du même niveau de protection sur tout le territoire de l'Union européenne. Et les mêmes devoirs s'appliquent simultanément à tous ceux qui gèrent les données personnelles de ces citoyens.

Vu l'étendue du champ d'application du GDPR (et des sanctions en cas de non-respect), il est plus que temps de vous informer et de vérifier si votre institution est en conformité.

Les conséquences du GDPR pour votre organisation

Dès le moment où vous traitez des données à caractère personnel, vous tombez dans le champ d'application du GDPR.

Ce chapitre aborde les grands principes du GDPR dont vous devez tenir compte. Il n'y a pas que les grandes multinationales ou les services commerciaux qui sont concernés. Les administrations publiques aussi. Et elles doivent se montrer exemplaires en la matière vis-à-vis du citoyen dont elles traitent les données personnelles au quotidien.

VOUS ÊTES RESPONSABLE !

Non seulement vous devez faire en sorte de vous conformer au GDPR, mais vous devez aussi démontrer que vous avez pris toutes les mesures appropriées. Vous ne pouvez donc pas vous reposer simplement sur vos sous-traitants.

REGISTRE DES DONNÉES ET ÉTUDE D'IMPACT

En tant que responsable ou sous-traitant du traitement[8] des données, le GDPR vous impose de **tenir un registre** qui mentionne le type de données, les finalités de ce traitement, les personnes concernées, la durée de conservation, les mesures de sécurité mises en place, etc.

Les données sont souvent dispersées auprès de différents services et sur divers supports (ordinateur, clé USB, serveur dans le cloud, dossiers papier...). Aucun de ces supports ne doit être oublié.

En ce qui concerne les données dites sensibles (lire page 12), vous devez aussi réaliser **une étude d'impact**, notamment sur les risques encourus dans le stockage ou le traitement de ces données.

8 Le GDPR définit le **responsable de traitement** comme toute personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données. Le **sous-traitant** est la personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement.

DÉSIGNEZ UN DATA PROTECTION OFFICER (DPO)

Les autorités publiques DOIVENT désigner un Délégué à la protection des données (DPO en anglais). Il est notamment chargé d'informer, de conseiller, de contrôler le respect de la réglementation[9].

Si vous ne disposez pas de quelqu'un en interne, le Règlement prévoit que la fonction peut être mutualisée entre plusieurs entités, y compris via un partenaire externe. Le CIRB peut donc endosser ce rôle pour votre administration (plus de détails en page 14).

DROIT À L'OUBLI ET À LA PORTABILITÉ DES DONNÉES

Le GDPR reprend des droits qui existaient déjà comme le droit pour chaque citoyen d'accéder, de corriger et de supprimer des données qui le concernent. Mais il en instaure aussi deux nouveaux : le droit à l'oubli et à la portabilité des données.

- **Le droit à l'oubli :** toute personne a le droit de vous demander de supprimer toutes les données dont vous disposez sur elle, même si elle vous a préalablement donné son consentement[10].
- **La portabilité des données :** à la demande d'un citoyen, vous devez lui transmettre, gratuitement et dans les 30 jours qui suivent sa demande, toutes les données personnelles qu'il vous a fournies à son sujet, « *dans un format structuré, couramment utilisé et lisible par une machine* », pour qu'elles soient ré-utilisables automatiquement par un autre service.

Il est donc important de prévoir dès à présent les modalités d'exercice de ces droits. Les données à supprimer ou à transmettre pouvant par exemple être dispersées auprès de plusieurs services différents. Et vous devez également être capable de démontrer le respect de ces obligations à l'autorité de contrôle.

9 Le DPO peut être une personne physique ou morale. Il/Elle est également le point de contact entre l'administration et l'autorité de contrôle. Il/Elle exerce avant tout une mission de conseil et de contrôle. Les décisions restent du ressort de l'administration.

10 Vous devez supprimer les données même si une disposition légale spécifique vous a autorisé à les collecter sans le consentement de la personne (à moins qu'une autre obligation légale vous impose de conserver ces données).

PRIVACY BY DESIGN / PRIVACY BY DEFAULT

Le GDPR introduit deux nouveaux concepts : la protection des données dès la conception (*privacy by design*) et la protection des données par défaut (*privacy by default*).

Ceci vous oblige à tenir compte de la vie privée et de la protection des données **dès la conception d'un nouveau produit ou service**. Les outils, comme un site Internet ou une application mobile, devront, par nature, respecter la vie privée. Le GDPR prévoit d'ailleurs de lourdes sanctions en cas de non-respect de ces principes.

DONNÉES SENSIBLES

Les données génétiques et biométriques sont ajoutées aux données dites sensibles comme l'origine ethnique, les opinions politiques ou les convictions religieuses.

Le traitement de ce type de données est interdit, hormis quelques exceptions ou si la personne concernée a explicitement donné son accord.

Notons que le GDPR octroie également une protection particulière aux données relatives aux enfants (lire page 17).

GESTION DES ACCÈS

Ne peuvent avoir accès aux données que les collaborateurs de votre institution qui en ont besoin. Pas question de laisser des fichiers en libre accès sur un serveur ou de se partager des listes d'adresses mail entre collègues.

Il est donc nécessaire de revoir la **gestion des accès aux données (Identity Access Management – IAM)**. Notamment quand une personne change de service, qu'il y a de nouveaux engagés ou des personnes qui quittent l'institution.

EN CAS DE VOL OU FUITE DE DONNÉES

On ne parle pas ici nécessairement d'un piratage informatique, mais de toute brèche dans la sécurité des données[11]. C'est le cas, par exemple, si on vole votre ordinateur ou des dossiers papier dans lesquels sont conservés des données à caractère personnel.

En cas de problème avec des données pouvant conduire à un risque pour les droits des personnes, vous devez **en avertir l'autorité de contrôle au plus tard dans les 72 heures** après avoir eu connaissance du problème. On ne parle pas ici de jours ouvrables, mais de jours calendrier (samedi, dimanche et jours fériés compris).

De plus, lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés de personnes physiques (usurpation d'identité, vol de numéro de carte de crédit…), vous devez aussi en informer les personnes concernées.

Réfléchissez dès maintenant aux procédures à mettre en œuvre : qui contacte l'autorité de contrôle, par quel(s) moyen(s), comment prévenir les personnes concernées, etc. C'est un vrai plan de communication de crise qu'il faut prévoir.

QUELLES SANCTIONS ?

La Commission de protection de la vie privée peut adresser des avertissements et des amendes en cas de non-respect du GDPR.

Pour les entreprises, ces amendes peuvent aller jusqu'à 4 % du chiffre d'affaires annuel mondial total ou 20 millions € (le montant le plus élevé étant retenu). Pour les organismes publics, les pays membres déterminent la nature et le montant des amendes.

En cas de préjudice, les personnes concernées pourraient aussi attaquer votre institution en dommages et intérêts.

Quoi qu'il en soit, outre la sanction pécuniaire, c'est aussi votre image de marque, votre réputation qui se verra écornée par d'éventuels avis négatifs de l'autorité de contrôle.

11 La violation de données est définie dans le GDPR comme une violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel.

Ce que le CIRB peut faire pour vous

Le CIRB a développé un service GDPR complet en cinq volets à destination de ses partenaires. **Vous pouvez faire appel à ces services dans leur ensemble ou à la carte, au travers d'un appel à ressources.**

Le CIRB s'est engagé depuis plusieurs mois dans la mise en conformité de ses propres services au travers d'un plan d'actions qui reprend ses obligations en tant que responsable ou sous-traitant de données à caractère personnel[12]. Pour ce faire, nous avons conçu **une série d'outils spécifiques** que nous mettons à votre disposition.

Cette mise en conformité au GDPR ne concerne pas uniquement les processus informatiques : il s'agit d'un projet transversal qui doit être porté par l'institution dans son ensemble.

ÉVALUATION PRÉALABLE

Le CIRB réalise un premier diagnostic et identifie les principaux types de traitement de données auxquels votre institution est confrontée et qui nécessitent une intervention au regard du GDPR.

Vous recevrez un rapport complet, incluant une estimation du risque et un plan d'actions.

12 Depuis 2010, le CIRB s'est doté d'un CISO (Chief Information Security Officer) en charge de la sécurisation des données et de la mise en conformité du Centre aux prescrits légaux. Son équipe réalise, sur demande, des missions similaires pour nos clients.

ACCOMPAGNEMENT DANS LA MISE EN CONFORMITÉ

Le CIRB peut affecter un chef de projet formé au GDPR qui vous accompagne dans tout le processus de mise en conformité de votre institution.

C'est une mission de conseil : le chef de projet CIRB déterminera avec vous les éléments à mettre en œuvre en priorité et assurera la coordination du plan d'actions. L'exécution de ce plan sera opérée par vos collaborateurs. Ce qui peut, le cas échéant, représenter un investissement opérationnel substantiel.

DPO AS A SERVICE

Le CIRB peut assurer le rôle de Data Protection Officer pour votre institution.

DPO COACHING

Si vous avez nommé un DPO en interne, le CIRB peut l'accompagner dans sa tâche.

Pour ces deux derniers services, nous avons constitué une équipe pluri-disciplinaire, avec des juristes et des experts de la sécurité informatique, qui se sont formés au GDPR.

FORMATIONS

Avec l'aide d'experts et de professeurs spécialisés en la matière, nous avons élaboré un programme de formations : de la conférence de 2h visant à conscientiser au GDPR jusqu'à une session complète de plusieurs jours.

Ce programme répond à la spécificité des services publics au regard de la nouvelle réglementation et englobe aussi toutes les fonctions concernées (administrative, juridique, informatique, communication...).

En resumé : un pense-bête en 10 étapes

1. INFORMER ET CONSCIENTISER

Le GDPR, c'est avant tout une gestion des risques : vous devez donc impliquer tous les collaborateurs de votre institution et les conscientiser à cette nouvelle réglementation.

2. REGISTRE DE TRAITEMENT

Etablissez dès maintenant un inventaire des types de données que vos services traitent, comment vous les conservez, avec qui vous les partagez, combien de temps vous les conservez, etc.

3. CHARTE VIE PRIVÉE

Rédigez ce document en y incluant tous les prescrits obligatoires du GDPR ou adaptez le texte si vous en avez déjà un.

4. CONSENTEMENT

Vérifiez que les consentements que vous avez déjà obtenus répondent aux nouvelles exigences du GDPR. A défaut, il vous faudra les redemander ou détruire les données que vous avez récoltées sans vous conformer à la nouvelle législation.

5. DROITS DE LA PERSONNE CONCERNÉE

Vos procédures internes permettent-elles de répondre aux citoyens qui feront usage de leurs droits d'accès, de modification, de suppression, d'effacement, de portabilité… dans le délai prévu par le GDPR ?

6. DATA PROTECTION OFFICER (DPO)

Désignez au plus tôt un délégué à la protection des données. Le CIRB peut endosser ce rôle, collaborer ou assister la personne qui assurera cette fonction au sein de votre institution.

7. ENFANTS

Le GDPR octroie une protection particulière aux données relatives aux enfants.
L'accord d'un parent ou d'un tuteur est obligatoire pour toutes les données concernant des enfants de moins de 16 ans. Attention donc si vous organisez, directement ou via un sous-traitant, de l'accueil extra-scolaire, des stages sportifs, etc.

8. FUITE DE DONNÉES

Prévoyez d'ores et déjà les procédures (notamment en communication) pour prévenir, détecter et réagir face à des brèches de sécurité, des pertes ou vols de données.
Le délai pour en avertir l'autorité de contrôle est assez court. Et dans certains cas, vous devrez aussi prévenir toutes les personnes concernées.

9. SOUS-TRAITANTS ET CONTRATS EXISTANTS

Répertoriez tous les sous-traitants qui interviennent sur des données à caractère personnel et adaptez les contrats qui vous lient au regard du nouveau règlement.

10. LE CIRB, VOTRE PARTENAIRE DE CONFIANCE EN MATIÈRE DE GDPR !

Contactez le CIRB pour vous assister dans le plan d'actions à mettre en œuvre au sein de votre organisation.

Ressources

Pour vous aider dans la mise en conformité de votre institution au GDPR, vous pouvez faire appel aux ressources suivantes :

- **Centre d'Informatique de la Région Bruxelloise (CIRB)**
  avenue des Arts 21 – 1000 Bruxelles
  02 282 47 70
  www.cirb.brussels
  Pour bénéficier des services GDPR du CIRB, contactez votre Account Manager via l'adresse: customer@cirb.brussels

- **Commission de protection de la vie privée (CPVP)**
  rue de la Presse 35 – 1000 Bruxelles
  02 274 48 00
  www.privacycommission.be

- Le site dédié spécialement au GDPR mis en ligne par la **Commission européenne** (en anglais) : www.eugdpr.org

cirb.brussels
IT is for you

ÉDITEUR RESPONSABLE :
Hervé Feuillien – Avenue des Arts 21 – 1000 Bruxelles