Guide du bon usage du Règlement général sur la protection des données (RGPD)

CRef
CONSEIL DES RECTEURS

fnrs
LA LIBERTÉ DE CHERCHER

Sommaire

Les termes utilisés sont entendus dans leur sens épicène, en sorte qu'ils visent les femmes et les hommes.

ÉDITO

Dès décembre 1992, la Belgique se dotait d'une loi *« Loi Vie privée »* dont l'objectif était de protéger le citoyen contre l'utilisation illégitime de ses données à caractère personnel. En 1995, le Parlement et le Conseil de l'Union européenne adoptaient une Directive 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.

Depuis, les données à caractère personnel ont pris de plus en plus de valeur jusqu'à devenir l'Or Noir du XXIe siècle, tandis que les évolutions techniques ouvrent de nouvelles possibilités d'exploitation de ces données. Il suffit d'observer l'attrait que les GAFAM (Google, Apple, Facebook, Amazon, Microsoft), pour ne citer que ces acteurs, ont pour collecter et utiliser ces données.

C'est en réponse à ces préoccupations qu'est né le Règlement général sur la protection des données (RGPD), qui est d'application depuis le 25 mai 2018.

Ce guide du bon usage du RGPD vous présente les grandes lignes de cette réglementation de manière simple et pratique, en se basant sur l'expérience de sa mise en application dans les universités représentées au Conseil des Recteurs, le CRef.

De quoi parle-t-on ?

Le RGPD s'applique à tous les traitements de données à caractère personnel. De quoi s'agit-il ?

Les données

Par *« donnée à caractère personnel »*, on entend toute information relative à un individu identifié ou identifiable. La définition est large puisqu'elle couvre tant des identifiants (tels les nom et prénom d'un individu) que toute information se rapportant à un individu que l'on a identifié (tels les résultats d'un examen d'un étudiant) ou à un individu dont nous n'avons pas l'identité mais qui pourrait être identifié raisonnablement (des images de vidéosurveillance, voire le son d'une voix, ou encore des données qui ont été codées). Par ailleurs, la combinaison de données non-identifiantes permet parfois d'identifier un individu, transformant ces informations amalgamées en données à caractère personnel.

Les données sensibles

Certaines données sont qualifiées de *« particulières » ou de « sensibles »*. Il s'agit des informations ayant trait à une origine ethnique, à la vie sexuelle, aux convictions religieuses ou philosophiques, aux opinions politiques, à l'affiliation syndicale, à la santé physique ou mentale ainsi que des données génétiques ou biométriques lorsque celles-ci sont utilisées pour identifier une personne. Leur traitement est interdit sauf dans le cadre d'exceptions et obéit alors à des règles plus strictes.

Les traitements

L'utilisation faite de ces données – normales ou sensibles – est nommée *« traitement »*. A nouveau, la portée de cette notion se veut très large et recouvre une ou un ensemble d'opérations, qu'elles soient automatisées ou non, effectuées sur ces données (depuis la collecte, l'enregistrement, la modification, l'utilisation jusqu'à et y compris la destruction des données) pour une ou plusieurs finalités (objectifs) déterminées.

Les transferts

Lorsque des données sont transférées à des personnes ne faisant pas partie de l'Université, des règles plus ou moins contraignantes s'appliquent. En particulier, le RGPD restreint le transfert de données en dehors du territoire de l'Union européenne. Des régimes d'exception existent, mais il faut privilégier tant que faire se peut une conservation des données au sein de l'Union européenne.

Qui est concerné ?

Le RGPD met en scène plusieurs acteurs.

Le responsable du traitement

Il s'agit de la personne (physique ou morale) qui, seule ou avec d'autres, détermine les finalités du traitement (le pourquoi) et les moyens utilisés pour le mettre en œuvre (le comment). Il lui incombe de s'assurer du respect des règles du RGPD, notamment par l'encadrement de son personnel.

Les Universités sont responsables du traitement.

Le sous-traitant

Il s'agit de la personne (physique ou morale) qui traite des données à caractère personnel pour le compte du responsable du traitement. Typiquement, il peut s'agir d'un prestataire technique dont l'objet du service est d'assurer des opérations techniques sur des données à la demande du responsable du traitement (voir page 9).

Les personnes concernées et leurs droits

Il s'agit des personnes physiques dont les données à caractère personnel sont traitées.

L'objectif du RGPD étant de donner davantage de contrôle aux individus sur leurs données à caractère personnel, plusieurs droits leur sont octroyés (voir page 10).

Le Délégué à la protection des données ou DPO

Grande nouveauté apportée par le RGPD, une fonction de Délégué à la protection des données (DPO, *Data Protection Officer*) est créée. Dans un certain nombre de cas, cette fonction est obligatoire au sein de l'organisme. Les universités francophones ont toutes désigné un DPO.

Le DPO est un acteur important de la mise en œuvre du RGPD. Il agit en tant qu'intermédiaire entre les acteurs concernés : l'Autorité de contrôle, les membres de la communauté universitaire et les personnes concernées. Il peut être consulté sur des questions ou des projets impliquant le traitement de données à caractère personnel (si possible dès leur conception).

L'Autorité de protection des données

Depuis le 25 mai 2018, la Commission de protection de la vie privée (CPVP) a été remplacée par l'Autorité de protection des données (APD). Il s'agit de l'Autorité de contrôle pouvant vérifier d'initiative la bonne application du RGPD ou recevoir les plaintes des personnes concernées relatives au traitement de leurs données.

Quelle mise en œuvre ?

Les principes à respecter dès la conception d'un traitement

Le RGPD repose sur six principes fondamentaux.

1. Chaque traitement doit avoir une des bases juridiques définies dans le RGPD et être mené de manière transparente pour les personnes concernées. A l'Université, les bases les plus souvent utilisées seront une obligation légale ou contractuelle, l'exercice des missions d'intérêt public ou encore le consentement (qui doit être explicite).
2. Les données ne peuvent être traitées que pour une ou plusieurs finalités déterminées et clairement annoncées.
3. Seules les données strictement nécessaires à la ou les finalités peuvent être traitées.
4. Les données doivent être exactes et, si nécessaire, tenues à jour.
5. Les données ne doivent pas être conservées au-delà du strict nécessaire pour la finalité du traitement (voir page 9).
6. La sécurité des données doit être assurée à l'aide de mesures techniques ou organisationnelles appropriées. Elle se décline en trois aspects : confidentialité / intégrité / disponibilité (voir pages 14 et 15).

L'Université doit, à tout moment, être en mesure de démontrer à l'Autorité de contrôle et aux personnes concernées que ces principes sont respectés, par exemple en documentant les mesures ou décisions prises pour en assurer le respect.

Durée de conservation

La définition de la durée de conservation des données est une exigence de base en matière de protection des données. Elle ne doit pas dépasser la durée nécessaire à la réalisation des finalités pour lesquelles les données sont traitées. Souvent, la législation précise elle-même cette durée.

Les aspects contractuels

Si l'Université fait appel à un prestataire externe (y compris un fournisseur d'application logicielle) pour traiter des données à caractère personnel pour son compte et sur ses instructions, elle doit s'assurer que ce dernier, qui aura la qualité de sous-traitant (voir page 6), tiendra compte des exigences du RGPD, en particulier pour ce qui concerne la sécurité et la confidentialité des données. Le RGPD impose également la conclusion d'un contrat écrit, qui doit obligatoirement régler certains aspects du traitement confié.

De même, si l'Université est amenée (par exemple dans le cadre d'un projet de recherche) à traiter des données pour le compte d'un tiers, elle doit également être couverte par un contrat.

Un contrat entre « *responsables conjoints* » pourra aussi être nécessaire en cas de recherche collaborative.

Quels devoirs pour l'Université ?

Le registre et l'information préalable

L'Université doit tenir un registre décrivant tous les traitements de données réalisés en son sein. L'APD peut demander à y accéder à tout moment. La collaboration du personnel est indispensable pour la création et le maintien à jour de cet outil, qui permet aussi de *mettre le doigt* sur des lacunes éventuelles.

Par ailleurs, l'Université doit indiquer aux personnes concernées, notamment, qui est le responsable du traitement, quelles en sont les finalités et les bases juridiques, qui peut accéder aux données, si les données sortent de l'UE et les coordonnées du DPO. Il faut se préoccuper de cette exigence au moment où l'on obtient ces données, qu'on les recueille directement auprès des personnes ou par un autre moyen.

Le respect des droits des personnes concernées

Le droit d'information ne se limite pas à une simple annonce initiale. Les personnes concernées peuvent demander, à tout moment, des informations complémentaires sur le traitement, sur les données utilisées ; en solliciter, entre autres, la rectification, l'effacement (droit à l'oubli) ou encore s'opposer à leur traitement.

Il convient donc de mettre en place une procédure permettant l'exercice effectif de ces droits et une réaction à une demande dans le délai légal d'un mois.

Quand mener une analyse d'impact ?

La gestion du risque

Les traitements de données à caractère personnel présentant des risques élevés pour les droits des personnes nécessitent une analyse de risques plus approfondie appelée analyse d'impact.

Si, à l'issue de cette analyse d'impact, le risque est jugé élevé, il peut y avoir obligation de consulter l'APD.

Seuls sont visés les traitements pouvant présenter un risque élevé pour les droits et libertés des personnes concernées tels que :

- Le droit au respect de la vie privée
- Le droit à la libre circulation
- La liberté de parole et d'information
- La liberté de réunion et d'association
- La liberté de pensée, conscience, religion
- Le respect du secret médical
- L'interdiction de discrimination
- Le droit à l'intégrité et dignité

Le RGPD donne quelques exemples, dont le profilage, le traitement à grande échelle de données sensibles ou l'utilisation d'une technologie nouvelle.

L'APD a publié une liste contenant d'autres exemples, tels que le traitement de données biométriques en vue de l'identification des personnes ou le traitement à grande échelle de données générées au moyen d'appareils dotés de capteurs.

En pratique, le DPO est là pour aider le responsable du traitement à déterminer si une analyse d'impact est nécessaire et comment la réaliser.

La recherche

Le RGPD s'applique au secteur de la recherche. Les traitements en matière de recherche devront donc se retrouver dans le registre (voir page 10).

Les rédacteurs du RGPD et le législateur belge ont prévu un régime spécifique pour concilier vie privée et liberté de recherche.

Des marges de manœuvre par rapport aux règles générales sont ainsi possibles en matière de recherche, principalement :

- la réutilisation de données (*« traitement ultérieur »*) est réputée compatible avec la finalité initiale ;
- les données peuvent être conservées plus longtemps que le régime ordinaire ;
- les données sensibles peuvent être traitées par le chercheur ;
- il est possible de déroger au droit à l'effacement et à l'oubli. Des dérogations aux autres droits ne sont possibles que moyennant l'application de la loi belge du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Des garanties appropriées doivent toutefois être prises, comme :

- la minimisation (ne traiter que les données strictement nécessaires) ;
- l'anonymisation si elle est possible ;
- la pseudonymisation (codage) ;
- le chiffrement des données ;
- la consultation d'un comité d'éthique ;
- le consentement de la personne concernée à participer au projet de recherche.

Comment mener les enquêtes par questionnaire ?

Concernant les enquêtes, il y a lieu de privilégier l'utilisation de techniques d'anonymisation, en particulier pour les enquêtes par questionnaire. En effet, si aucune donnée personnelle n'est traitée, la réglementation sur la protection des données à caractère personnel ne s'applique pas. Il s'agira toutefois de veiller à ce que les données soient réellement rendues anonymes, c'est-à-dire qu'on ne puisse établir aucun lien entre les réponses aux questions de l'enquête et la personne qui y participe.

Si ce n'est pas possible et que des données à caractère personnel doivent être collectées, il convient alors d'exposer clairement aux participants l'objet de l'étude et de leur fournir tous les éléments d'information requis par le principe de transparence. Cette information interviendra avant le début du traitement. La personne chargée de cette enquête conservera la preuve que cette information a été fournie.

Comment garantir la sécurité des données ?

Des mesures techniques permettent de s'assurer que le traitement de données à caractère personnel est conforme au RGPD.

Transfert et publication d'informations et de données

La confidentialité des données à caractère personnel doit être respectée, ce qui impose notamment de ne pas les transférer à des personnes qui n'ont pas besoin d'en prendre connaissance.

Les postes de travail

Les postes de travail qui seront utilisés pour traiter ces données doivent notamment être sécurisés dans le meilleur état de l'art et de la technique. Ils doivent être équipés d'antivirus et bénéficier automatiquement des mises à jour. Les sessions de travail doivent être protégées par un identifiant personnel et un mot de passe.

Un bon mot de passe

L'accès aux données à caractère personnel ne devrait se faire qu'après l'authentification de l'utilisateur, le plus fréquemment par l'utilisation d'un identifiant personnel et d'un mot de passe. Celui-ci doit être suffisamment complexe et strictement personnel.


COMME JE N'AI PAS DE MÉMOIRE, J'AI POSTÉ MON CODE SUR FACEBOOK POUR L'AVOIR PLUS FACILEMENT SOUS LA MAIN !!
AH ?! ...ET TES 2759 AMIS FACEBOOK ONT SÛREMENT DÛ LIKER CELA ?!

Comment stocker les données ?

Le stockage des données

Les données à caractère personnel doivent être stockées de manière sécurisée. Un espace de stockage *« institutionnel »* mis à la disposition par l'Université est recommandé. Cet espace peut prendre la forme d'un stockage local, d'un Cloud interne ou externe.

Le stockage de données à caractère personnel sur des postes de travail locaux, des solutions Cloud gratuites ou des supports amovibles comme des clés USB ou des disques durs externes est déconseillé, à moins que des mesures spécifiques de protection ne soient mises en place, comme le chiffrement des données.

Les données à caractère personnel doivent être sauvegardées sur un support de backup, lui-même sécurisé.

Les locaux physiques où sont stockées des données à caractère personnel doivent être sécurisés, fermés à clefs ou sous contrôle d'accès. Il en est de même pour les armoires où sont stockés des documents papiers ou des supports informatiques amovibles.

Fin de vie des informations

Lorsque des données à caractère personnel atteignent l'échéance de leur durée de conservation telle que déclarée dans le registre des traitements, elles doivent être détruites (voir page 9). S'il s'agit de données sous forme papier, elles devraient être broyées.

La gestion des incidents

Qu'est-ce qu'un incident ?

Un incident relatif à des données à caractère personnel est tout évènement qui résulte de la perte, du vol, de la destruction, des dégâts d'origine accidentelle ou de la modification non légitime de telles données, tel que le vol d'un ordinateur, le piratage d'un compte ou d'un mot de passe ou la perte d'une clé USB.
L'accès non autorisé ou illicite constitue également un incident.

Que faire en cas d'incident ?

Selon leur gravité, ces incidents sont à notifier à l'APD dans les 72 heures suivant leur détection, par l'Université comme responsable du traitement, ou, par délégation, par son DPO. Pour que cette obligation soit remplie, il est indispensable que tous les membres de la communauté universitaire acquièrent le réflexe de communiquer immédiatement les incidents qu'ils constatent selon la procédure mise en place au sein de l'Université.

Les bons réflexes

En pratique, signalez immédiatement, selon les procédures définies par votre Université :

- la perte ou le vol d'équipement informatique : clé USB, ordinateur portable, gsm, etc. ;
- l'abandon dans un lieu public de données à caractère personnel sous format papier : fardes, dossiers, etc. ;
- la perte ou vol de dossiers papiers contenant des données à caractère personnel ;
- un mot de passe ou un login compromis : par diffusion, hacking, hameçonnage, etc. ;
- tout autre incident impliquant des données à caractère personnel.

Si l'Université ne respecte pas ses obligations de notification des incidents de sécurité, elle s'expose à des sanctions de l'APD.

Conclusion

Si le RGPD crée de nouvelles obligations, il renforce essentiellement des exigences qui existaient déjà légalement mais n'étaient pas toujours connues de tous.

Le respect du RGPD par l'Université nécessite l'implication de son personnel, par exemple pour participer à la tenue du registre des activités de traitement, garantir la sécurité des données ou signaler les incidents relatifs aux données.

Votre DPO est là pour vous conseiller. Le cas échéant, il pourra vous aiguiller vers des correspondants techniques spécialisés en matière de protection des données.

Le RGPD a permis, en fin de compte, de faire comprendre la valeur de nos données à caractère personnel et l'importance de les protéger dans un cadre légal renforcé.

Ne passons pas à côté d'un sujet aussi sensible !

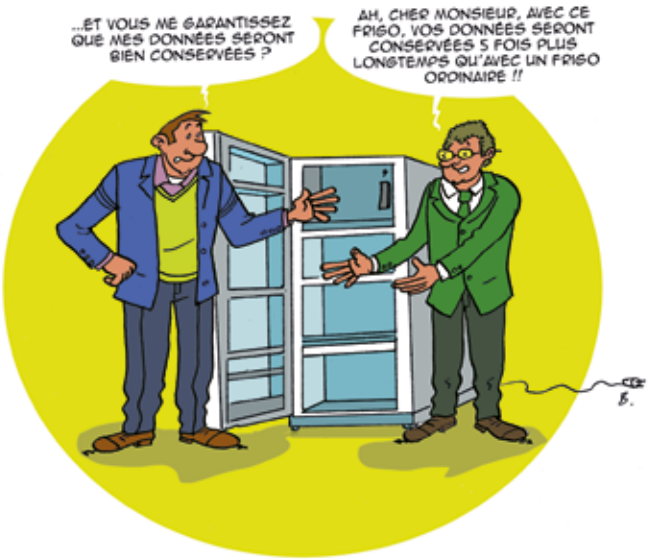
Merci d'avance pour votre collaboration.

Pour en savoir plus...

➔ Règlement général sur la protection des données:
https://www.autoriteprotectiondonnees.be/le-règlement-général-sur-la-protection-des-données-rgpd

➔ Autorité de protection des données:
https://www.autoriteprotectiondonnees.be/

➔ European Data Protection Board (Autorité de contrôle européenne): **https://edpb.europa.eu/**



ULB – ULiège – UMONS – UCLouvain – UNamur – USL-B

Éditeur responsable: Vincent Blondel, CRef, Rue d'Egmont, 5 - 1000 Bruxelles. Mai 2019 • Illustrations: Baloo • Graphisme: by-im.be