RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES - RGPD

GENERAL DATA PROTECTION REGULATION - **GDPR**

Cette réglementation est entrée en vigueur le 25/05/2016. Une période transitoire de 2 ans a été prévue et celle-ci sera d'application effective à partir du 25 mai 2018.

ASSOCIATION DES ÉTABLISSEMENTS SPORTIFS

Ce document synthétique a été rédigé par l'Administration commune AES - AISF et est une première approche pour la mise en place du RGPD.

Réalisé par Sophie Denooz

La règlementation sur la protection de la vie privée n'est pas quelque chose de nouveau. Le cadre actuel est la Directive UE 95/46 et celle-ci est transposée en droit belge par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Cette directive sera abrogée et remplacée par le Règlement 2016/679 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données. Ce règlement est directement applicable dans chacun des états membres de l'Union européenne.

ÊTES-VOUS CONCERNÉ PAR CE NOUVEAU RÈGLEMENT ?

Le GDPR sera d'application à toute entité légale collectant des données personnelles, autant pour le secteur marchand que pour le secteur non marchand. L'Union européenne n'a pas limité ces nouvelles règles uniquement au secteur des sociétés, mais il sera bel et bien d'application pour toutes les organisations. L'UE a voulu faire valoir ces nouvelles règles pour tous ceux qui traitent des données. Évidemment, les personnes physiques qui conservent des données à des fins privées ne sont pas soumises à ce règlement. Par contre, les centres sportifs, les fédérations sportives et les clubs sportifs qui gèrent des données concernant les membres des clubs, les membres des Conseils d'administration, les membres du personnel… seront, quant à eux, soumis aux dispositions édictées par ce règlement.

I. CHAMP D'APPLICATION

Le champ d'application est le même que dans l'ancien règlement.

Le champ d'application est repris à l'article 2 du GDPR : *« Le présent règlement s'applique au traitement des données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »*

RAPPEL DE QUELQUES CONCEPTS DE BASE

Ces concepts sont définis à l'article 4 du GDPR.

1. **Traitement** = *« Toute information ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. »*
2. **Données à caractère personnel** = *« Toute information se rapportant à une personne physique identifiée ou identifiable […]. »*

   Il existe trois catégories particulières de données : cela a un impact sur le consentement ou les conditions dans lesquelles le traitement de ces données va pouvoir être effectué. Cette différenciation existait déjà dans la précédente législation.

   - Données **sensibles** (opinion politique, orientation sexuelle…). Ces données font l'objet d'un traitement particulier qui aura une conséquence sur le consentement.
   - Données relatives à la **santé**.
   - Données **judiciaires** (c'est la catégorie la plus protégée, normalement elles ne peuvent être demandées que si une base légale l'autorise).

3. **Responsable du traitement** = *« La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement [...]. »*

   Cette personne décide notamment quelles sont les données à récolter et le pourquoi. Si on applique cela à la relation de travail, c'est en général l'employeur.

4. **Sous-traitant** = *« La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. »*

II. PRINCIPES GÉNÉRAUX

Les principes généraux relatifs au traitement des données sont l'essence même de ce règlement.

Pour rappel, ces derniers sont les suivants :

- ☛ Licéité (conforme à la législation), loyauté (une fois les buts définis, les données doivent être traitées comme telles), transparence (le but doit être connu).
- ☛ Limitation des finalités (les données doivent être collectées pour des finalités déterminées).
- ☛ Minimisation des données (les données traitées doivent être adéquates et pertinentes à ce qui est nécessaire, on ne peut pas récolter des données par anticipation).
- ☛ Exactitude (les données peuvent être modifiées lorsqu'elles ne sont pas correctes).
- ☛ Limitation de la conservation des données dans la durée[1].
- ☛ Intégrité et confidentialité (les données doivent être protégées).

III. LES CHANGEMENTS

1. LE CONSENTEMENT

Le consentement n'est pas nouveau, mais il sera dorénavant plus strict par rapport au consentement donné par le titulaire des données.

Consentement = *« toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement[2] »*.

Dorénavant,

- ☛ La demande de consentement sera formulée en des termes compréhensibles, accessibles et simples (informer clairement la personne des données récoltées, du pourquoi et du comment).
- ☛ Le consentement sera éclairé (c'est-à-dire après information claire et complète de la personne concernée sur les caractéristiques et modalités du traitement).
- ☛ Le consentement sera explicite.

La personne devra être informée clairement des données qui sont récoltées, du pourquoi ces données sont récoltées et du comment ces données vont être utilisées. La personne concernée acceptera de donner son consentement par une déclaration ou un acte positif clair.

---

1 Pour plus d'informations sur la durée de la conservation : https://www.privacycommission.be/fr/faq-page/10030#t10030n19814

2 Règlement (UE) 2016/679, article 4, 11).

★ **Exemple :** document individuel à faire signer aux travailleurs où ces derniers autorisent le traitement de leurs données.

De plus, il faut savoir que lorsqu'un traitement sera légitimé par le consentement explicite de la personne concernée, ce consentement pourra être retiré à tout moment. Cela ne voudra pas dire que tout le traitement des données qui a été fait jusqu'au retrait du consentement sera nécessairement illicite, mais ça signifiera que pour le futur on ne pourra plus se baser sur ce consentement pour traiter les données et donc les utiliser.

Il est conseillé d'utiliser, en plus du consentement, une base juridique supplémentaire. Si le consentement est retiré et qu'on n'a pas de base juridique, les données ne pourront plus être utilisées.

📎 **Infos :** https://www.privacycommission.be/fr/faq-page/10027

2. DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPD)

Le rôle du DPD sera de veiller à ce que le traitement des données soit conforme au nouveau règlement (proportionnalité, délai raisonnable...).

C'est obligatoire pour :

☛ Les organismes publics.

☛ Le traitement à grande échelle de données particulières ou judiciaires.

☛ Le traitement qui, du fait de sa nature, de sa portée ou de ses finalités, exige un suivi régulier et systématique à grande échelle des personnes concernées.

En dehors de ces trois hypothèses, ce DPD sera facultatif.

📎 **Infos :** https://www.privacycommission.be/fr/dossier-thematique-delegue-a-la-protection-des-donnees

3. CONFIDENTIALITÉ DÈS LA CONCEPTION ET PAR DÉFAUT

Il y a confidentialité dès la conception du traitement. Toutes les données qui sont récoltées doivent être évidemment confidentielles.

Ce qui est défini de manière plus claire maintenant, c'est que cette notion de confidentialité des données concernées est maintenant présente par défaut. C'est maintenant la règle de base, là où, avant, c'était optionnel. C'est plus un changement technique, cela ne va pas changer grand-chose par rapport au quotidien.

★ **Exemple :** lorsque vous avez une fiche de paie à jeter. Y a-t-il une procédure particulière pour la détruire au lieu de la mettre dans la corbeille à papier ?

4. VIOLATION DES DONNÉES

La violation des données est une nouvelle règle.

Il y aura une obligation de notification à la CPVP et à la personne concernée lors d'une infraction comme la destruction, la perte, l'altération ou la divulgation de données à caractère personnel.

Le responsable du traitement informe la commission de la vie privée dans les meilleurs délais et, si possible, 72 heures au plus après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Le responsable du traitement informe aussi la personne concernée dans les meilleurs délais lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

★ **Exemple :** une photo prise à la fête du personnel est publiée, il n'y aura pas d'impact. Par contre une donnée judiciaire, comme le certificat de bonne vie et mœurs, c'est autre chose.

La notification devra reprendre la description de l'incident, les conséquences et les mesures prises afin de remédier à la violation.

📎 **Infos :** https://www.privacycommission.be/fr/faq-page/10521

5. OBLIGATION D'INFORMATION ET DE TRANSPARENCE

Ce principe n'est pas nouveau, mais il est plus explicite.

La personne dont les données seront traitées doit être informée de :

☛ La durée du délai de conservation
📎 **Infos :** https://www.privacycommission.be/fr/faq-page/10030#t10030n19814.

☛ Si un envoi des données à caractère personnel est prévu hors de l'UE.

☛ La base juridique.

☛ La possibilité d'introduire une réclamation auprès de la Commission de la protection de la vie privée.

6. OBLIGATION DE TENIR UN REGISTRE DE DONNÉES

Ce changement remplace l'obligation de déclaration à la CPVP.

Les traitements effectués dans l'entreprise ou l'association seront consignés dans un registre. Ce registre sera tenu à la place de la déclaration d'un registre des activités de traitement à la CPVP.

Pour qui est-ce obligatoire ?

☛ Lorsqu'il y a plus de 250 travailleurs.

☛ Lorsqu'il y a un risque de violation de la confidentialité.

☛ Lorsqu'il y a un traitement régulier de données personnelles.

☛ Lorsqu'il y a une utilisation particulière de données.

Si l'association ou entreprise ne rentre pas dans ces conditions, la CPVP recommande malgré tout d'établir un registre.

Le registre peut être conservé sous format électronique et ne doit pas être fourni à la CPVP.

★ **Exemple :** il faudra indiquer dans ce registre s'il y un contrôle des emails, un contrôle de page internet, s'il y a une surveillance caméra, les données pour le traitement de la paie…

En établissant le registre, il faut en profiter pour faire l'inventaire des données que vous récoltez. Sont-elles indispensables pour le but de la récolte ? Par exemple, la récolte d'une donnée relative à la santé d'un individu n'est pas toujours nécessaire.

📎 **Infos :** https://www.privacycommission.be/fr/registre-des-activites-de-traitement

La CPVP a mis un modèle de registre en ligne :
https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

7. DONNÉES SENSIBLES

Certaines données font l'objet d'une attention renforcée. Il existe deux catégories : les données particulières et les données judiciaires.

☛ **Données particulières**

- origine raciale ;
- opinion politique ;
- opinion religieuse ;
- données génétiques ;
- appartenance syndicale ;
- opinion philosophique ;
- données sur la santé ;
- données biométriques ;
- données sur l'orientation sexuelle.

Le GDPR prévoit que le traitement de ces données est interdit. Néanmoins, il existe des exceptions. Si le traitement d'une donnée particulière doit avoir lieu, il faut vérifier si l'exception est applicable.

★ **Exemple :** L'interdiction pourra être levée si la personne concernée donne son consentement explicite (sauf s'il est prévu légalement que cette interdiction ne peut être levée).

☛ **Données judiciaires :** données relatives aux infractions, aux condamnations pénales…

Le traitement de ces données ne peut être effectué qu'à certaines conditions : le traitement est effectué sous le contrôle de l'autorité publique ou le traitement est autorisé par la loi.

8. TRANSFERT VERS DES PAYS TIERS

Cette condition était déjà fixée, mais elle est renforcée. Il pourra y avoir un transfert des informations en dehors de l'Union européenne uniquement si le pays est reconnu par la Commission européenne comme pays disposant d'une protection adéquate concernant la protection des données ou dans des circonstances particulières, avec les mesures de protection nécessaires.

📎 **Infos :** https://www.privacycommission.be/fr/faq-page/10178

9. LES DROITS DE LA PERSONNE CONCERNÉE

Cette règle n'est pas nouvelle, mais elle est plus étendue, les droits sont précisés.

☛ **Droit d'opposition** : interdiction de continuer à traiter les données pour autant que l'on se trouve dans un cas où le traitement des données repose sur le consentement.

Cela n'est pas possible lorsque c'est nécessaire à l'exécution d'un contrat ou nécessaire à l'accomplissement d'obligation légale.

★ **Exemple :** Un travailleur ne peut interdire d'utiliser des données qui pourraient induire l'arrêt de sa paie.

☛ **Droit de rectification :** possibilité de faire corriger les données incorrectes ou de compléter ces données.

☛ **Droit d'accès :** Le titulaire des données peut connaître les données conservées à son égard, pourquoi elles sont conservées, le destinataire éventuel de ces données… Désormais, il est ajouté : la durée de conservation, si les données sont envoyées en dehors de l'UE ou non et la possibilité d'introduire une réclamation.

☛ **Droit à l'effacement des données :** Lorsque la finalité du traitement des données a disparu, le titulaire des données peut demander que ces données soient effacées sauf si action en justice ou droits de tiers.

☛ **Droit à la limitation du traitement :** Le titulaire des données à droit à la limitation du traitement dans certaines hypothèses précisées par le règlement. Si c'est le cas, le responsable du traitement ne pourra alors traiter les données du titulaire qu'avec le consentement de celui-ci ou pour des motifs spécifiques comme par exemple une action en justice.

☛ **Droit à la portabilité des données :** La possibilité de transférer les données personnelles d'un responsable de traitement à un autre. Exemple : changement d'employeur.

☛ **Droit d'introduire une réclamation :** Le droit d'introduire une réclamation à la Commission de la vie privée doit être communiqué explicitement au travailleur.

☛ **Droit d'obtenir une copie :** Il a été ajouté que la copie des données personnelles pouvait se transmettre sous forme électronique.

10. RISQUE DE SANCTION PLUS ÉLEVÉE

Le risque de sanction plus élevée est une nouveauté instaurée par ce règlement.

☛ **Renversement de la charge de la preuve :** Il y a un renversement de la charge de la preuve. Autrefois, c'est le travailleur qui devait prouver le fait que la façon dont ses données étaient transmises n'était pas correcte. Désormais, il appartiendra à l'employeur de prouver le respect des règles édictées par le règlement. C'est donc l'une des raisons pour laquelle le registre de données est important.

☛ **Pouvoir de sanction de la Commission de la protection de la vie privée :** La Commission de la protection de la vie privée va disposer d'un pouvoir de sanctions à l'encontre des organisations qui ne satisfont pas aux règles édictées par le règlement. C'est un système de sanctions échelonnées. Ces sanctions peuvent varier du simple avertissement à l'amende administrative si l'organisation n'obtempère pas ou si elle ne se met pas en ordre dans les délais qui lui sont impartis.

- Avertissement ou rappel à l'ordre.
- Obligation de mettre le traitement en conformité.
- Accéder à la demande d'exercice des droits ou notifier l'infraction au travailleur.
- Limitation temporaire ou définitive du traitement.
- Amende administrative.

La CPVP aura du mal à tout contrôler, mais un travailleur a le droit d'aller se plaindre et la Commission pourra s'intéresser à cette entreprise ou association par ce biais-là.

IV. PRÉPARATION AU GDPR

La Commission de protection de la vie privée a édité une brochure ***« RPGD : préparez-vous en 13 étapes ».***

Vous trouverez ci-dessous un résumé.

- *« Conscientisation : il s'agit de conscientiser les personnes-clés et les décideurs aux changements importants en matière de données à caractère personnel qui se dessinent pour mai 2018.*
- *Établissement d'un registre de données : il est recommandé de faire un inventaire minutieux des données traitées, de noter leur provenance, les personnes avec lesquelles elles sont partagées ainsi que leur fondement légal.*
- *Communication : le responsable de traitements doit communiquer à chacune des personnes concernées ses droits ; cela se fait par une déclaration de confidentialité qui devra être mise à jour au regard des nouvelles obligations du règlement.*
- *Gestion des droits de la personne concernée : il s'agit d'examiner si la façon de traiter les données respecte les (nouveaux) droits de la personne concernée.*
- *Gestion des demandes d'accès : la Commission conseille de réfléchir sur la manière de gérer les demandes d'accès aux données par les personnes concernées.*
- *Déterminer le fondement légal du traitement de données à caractère personnel.*
- *Évaluer la qualité du consentement lorsqu'il s'agit du fondement légal du traitement utilisé et adapter les procédures aux nouvelles obligations du règlement.*
- *Évaluer et adapter les procédures en offrant aux enfants une protection spécifique.*
- *Détection et gestion des fuites de données : il s'agit de déterminer les risques de fuites de données, leur gestion et la mise en place d'une procédure en cas de notification à l'autorité de contrôle.*
- *Protection des données dès la conception et analyse d'impact : veiller, dès le début, à prévoir une conception des traitements des données qui permette le respect du nouveau règlement et envisager la réalisation d'une analyse d'impact.*
- *Désignation d'un délégué à la protection des données si nécessaire.*
- *Au niveau national, déterminer l'autorité de contrôle compétente et si les opérations de traitement ont un caractère national.*
- *En ce qui concerne les contrats existants et futurs, évaluer et mettre en conformité les relations contractuelles avec vos sous-traitants[3]. »*

Infos : https://www.privacycommission.be/sites/privacycommission/files/documents/STAP-PENPLAN%20FR%20-%20V2.pdf

3 RGPD – Nouveau règlement européen en matière de protection de la vie privée en quelques mots. Marie-Laure Van Rillaer. Union des Villes et Communes de Wallonie

V. QUELQUES CAS PRATIQUES

Afin d'illustrer la théorie, vous trouverez ci-après quelques exemples qui pourraient s'appliquer au sein de votre centre sportif, fédération sportive ou club sportif. Cette liste ne se veut pas exhaustive car il appartient à chaque entité de se mettre en conformité avec la législation selon son environnement.

★ **Exemples :**

- **Un club de tennis organise un tournoi. Pour ce faire, le participant doit s'inscrire via un formulaire sur internet où on lui demande ses coordonnées, son classement, ...** Que doit faire le club ? En dessous du formulaire que le participant doit compléter, il doit y avoir un endroit prévu pour qu'il marque son accord, et doit donc accepter que ces données soient utilisées. Le club va devoir mentionner les données récoltées, la finalité et la durée de la conservation des données.
- **La fédération de basket publie tous les 3 mois un magazine sur l'actualité du basket en Belgique et en Europe. Dans ce magazine, il y a des photos de participants à une formation qu'elle avait organisée**. Pour pouvoir publier une photo d'un participant dans son magazine, la fédération doit obtenir le consentement de la ou des personne(s) concernée(s). Le consentement ne pourra pas être oral, il devra être éclairé et explicite. Une des possibilités est, par exemple, de donner un document au(x) participant(s) lors de l'inscription de cette personne où celle-ci devra marquer ou non son accord pour la publication de la photo dans le magazine. Il faudra bien expliquer le but de la collecte des photos.
- **Le centre sportif de Waremme engage le mois prochain un nouveau sauveteur pour sa piscine.** Il va lui faire signer un contrat de travail mais également une convention « vie privée ». Cette dernière devra être signée par le travailleur et l'employeur. Cette convention reprendra notamment les données du travailleur dont l'employeur a besoin (avec le délai de conservation, les destinataires et les finalités), les droits du travailleur (droit d'accès, droit de rectification, ...) la procédure en cas de violation, le consentement.

SOURCES

☛ Règlement du 27 avril 2016 relatif à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

☛ https://www.privacycommission.be

☛ *« GDPR : Que devez-vous savoir ? »*
SECUREX

☛ *« Le Règlement général sur la Protection des Données (RGPD) en 10 leçons. »*
Laure LANDES-GRONOWSKI Avocate associée, Avistem Avocats.

☛ *« Le nouveau règlement sur la protection des données et ses conséquences pour les entreprises en Belgique »*
Fédération des Entreprises de Belgique.

☛ *« RGPD – Nouveau règlement européen en matière de protection de la vie privée en quelques mots. »*
Marie-Laure Van Rillaer. Union des Villes et Communes de Wallonie.