GUIDE PRATIQUE :
LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (RGPD)

Entrée en vigueur : 25 mai 2018

Ce document de travail a été réalisé sur base du croisement des deux documents émis par la Commission de la protection de la vie privée suivants :
- *« RGPD - Préparez-vous en 13 étapes »*
- *« Vade-mecum pour les PME »*

Il est émis à titre purement indicatif par l'Agence culturelle de Wallonie picarde, Culture.Wapi pour ses partenaires.

Ce document n'est pas exhaustif. Il est volontairement synthétique et il est vivement conseillé de consulter l'intégralité des textes d'origine susmentionnés pour une parfaite information.

Liens utiles :
- *Texte intégral du règlement général sur la protection des données*
- *Site de la Commission de la protection de la vie privée belge*

SOMMAIRE

1. PRINCIPES DE BASE
   - 1.1. Le RGPD : Pour qui ?
   - 1.2. Qu'est-ce qu'une donnée à caractère personnel ?
   - 1.3. Qu'est-ce qu'un traitement de données à caractère personnel ?
   - 1.4. Les principes généraux du RGPD
   - 1.5. Sanctions

2. COMMENT SE METTRE EN CONFORMITÉ AVEC LE RGPD ?
   (Quelques clés des 13 étapes établies par la Commission de la protection des données)
   - 1ère étape : Conscientisation
   - 2ème étape : Tenir un registre des activités de traitement
   - 3ème étape : Désignation d'un délégué à la protection des données
   - 4ème étape : Cas pratique - les newsletters
   - 5ème étape : Droits de la personne concernée
   - 6ème étape : Sécurité

1. PRINCIPES DE BASE

1.1. LE RGPD : POUR QUI ?

Le règlement général à la protection des données ne fait pas de distinction entre les secteurs public ou privé, marchand ou non-marchand. Dès lors, le RGPD est l'affaire de tous : grandes ou petites entreprises, associations sans but lucratif, coopératives, travailleurs indépendants, etc.

Le règlement est d'application dès qu'une organisation possède des données à caractère personnel (1.2.) **ET** effectue un traitement de ces données (1.3).
Autrement dit, il est plus que probable que ce nouveau Règlement vous concerne tous.

Il est important de déterminer les acteurs auxquels s'applique le RGPD :

- **Responsable du traitement** : L'instance qui détermine les finalités et les moyens du traitement = Culture point wapi, le musée X, le Centre culturel Y, l'asbl Z, etc.
- **Sous-traitant** : L'entreprise qui traite des données à caractère personnel pour le compte d'un responsable du traitement = OVH, Mailchimp, Google, service cloud, etc.
- **Personnes concernées** : Les personnes identifiables ou identifiées dont des données à caractère personnel sont traitées = Clients, publics, adhérents, visiteurs, membres du personnel, etc.

Remarque : **Approche basée sur les risques**
Les obligations qui découlent du RGPD varient en fonction du risque lié à l'activité de traitement (volume et sensibilité des données traitées). Même si le RGPD est l'affaire de tous, si vous traitez peu de données à caractère personnel, que la collecte de données n'est pas au cœur de votre activité et que le risque est peu élevé, le travail à fournir sera moins conséquent et exigeant que pour une grande entreprise ayant en sa possession des quantités astronomiques de données. Pas de panique donc !
Il est cependant intéressant de s'interroger sur ses pratiques en matière de protection des données. Montrer votre volonté et votre bonne foi constitue déjà un premier pas vers la mise en conformité avec le RGPD.

1.2. QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL?

- **Données à caractère personnel** : « toute donnée se rapportant à une personne physique identifiée ou identifiable » (article 4.1 du RGPD).
- Lorsque le couplage d'éléments d'information (âge, sexe, code postal, etc.) peut conduire à l'identification unique d'une personne ('singling out'), chaque élément constitue également une donnée à caractère personnel.

Exemples de données à caractère personnel :

- Données d'identification (nom, prénom, adresse, tél., …) ;
- Données d'identification électronique (adresses mail, adresses IP, cookies, ...) ;
- Données de localisation électronique (GSM, GPS, ...) ;
- Caractéristiques personnelles (âge, sexe, état civil, profession ...) ;
- Données physiques (taille, poids, ...) ;
- Photographies, images vidéo ;
- Habitudes de vie.

A contrario, ne sont pas des données à caractère personnel :

- Adresse e-mail générale ou numéro de téléphone général d'une structure (Ex. contact@culturepointwapi.be) ;
- Numéro d'entreprise (sauf dans le cas d'une entreprise unipersonnelle) ;
- Données anonymes ;
- De plus, le RGPD ne s'applique pas aux données relatives à des personnes décédées ou de personnes morales.

• **Les données sensibles** sont les données à caractère personnel qui méritent un niveau de protection plus élevé car leur traitement peut entraîner des risques significatifs. Le traitement de données sensibles est **en principe interdit**, à moins que vous ne satisfassiez à l'un des motifs d'exception de l'article 9 ou de l'article 10 du RGPD. Des données à caractère personnel ordinaires vous permettant de déduire des informations sensibles constituent également des données sensibles.

Exemples de données sensibles :
- Données relatives à la santé, les données génétiques et les données biométriques en vue de l'identification unique d'une personne ;
- Données à caractère personnel qui révèlent l'origine raciale ou ethnique, la vie sexuelle ou l'orientation sexuelle, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ;
- Données judiciaires relatives aux condamnations pénales et aux infractions.

1.3. QU'EST-CE QU'UN TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL?

La **notion de traitement** est très large et comprend toute opération effectuée ou non à l'aide de procédés automatisés et appliquée à des données à caractère personnel (article 4.2 du RGPD).

Un traitement de données à caractère personnel correspond notamment à :
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 des données.

Remarque : Bien que le RGPD vise principalement les traitements automatisés de données à caractère personnel (comme l'enregistrement sur un support numérique), vous ne pouvez pas contourner la loi en conservant toutes les données à caractère personnel sur des supports papier. La conservation sur papier de fichiers systématiquement organisés constitue également un traitement au sens du RGPD.

1.4. LES PRINCIPES GÉNÉRAUX DU RGPD

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

Ces principes 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). Ex. Si vous avez besoin des coordonnées de différentes personnes pour effectuer un envoi postal, il n'est pas nécessaire de leur demander également leur date de naissance pour une potentielle utilisation future.
- **Exactitude** (les données peuvent être modifiées lorsqu'elles ne sont pas correctes).
- Limitation de la **conservation** des données dans la **durée**.
- **Intégrité** et **confidentialité** (les données doivent être protégées).

1.5. SANCTIONS

L'Autorité de Protection des Données (Commission de la protection de la vie privée) peut imposer différentes sanctions en cas de non-respect du RGPD. Dans le cadre d'une réclamation ou de sa propre initiative, l'APD peut notamment :

- Donner un avertissement ou formuler un rappel à l'ordre ;
- Obliger à satisfaire à la demande de la personne concernée ;
- Obliger à mettre le traitement en conformité avec le RGPD dans un délai déterminé ;
- Geler ou interdire le traitement ;
- Infliger des amendes jusqu'à 2 % ou 4 % du chiffre d'affaires annuel, en fonction de la violation.

Toute organisation a une obligation de coopérer en cas d'enquête éventuelle de l'APD (article 31 du RGPD).

La responsabilité implique qu'un responsable du traitement doit pouvoir démontrer le respect du RGPD en cas de contrôle. Dès lors, la documentation des choix est primordiale de manière à ce qu'une organisation puisse justifier les raisons pour lesquelles elle a ou non instauré une mesure déterminée.

2. COMMENT SE METTRE EN CONFORMITÉ AVEC LE RGPD ?

La Commission de la protection de la vie privée a émis un guide en 13 étapes pour se préparer à l'arrivée du RGPD. Nous reprendrons les points qui nous semblent les plus pertinents dans notre situation et en ajouterons certains tout en essayant d'expliciter au mieux et de manière concrète les actions qui doivent être mises en place avant le 25 mai 2018. Voici quelques étapes clés :

1ère ÉTAPE : CONSCIENTISATION

Conscientisez l'ensemble de vos collaborateurs à la notion de protection des données. Son respect doit être partagé par tous. Il est intéressant de se questionner en équipe sur les pratiques et les mesures à adopter pour respecter au mieux le nouveau Règlement.

Il est important de documenter le fait que vous vous soyez penchés sur la problématique du RGPD et que vous ayez fait votre possible pour le respecter au mieux. Prévoyez une farde dans laquelle vous documenterez les démarches que vous aurez effectuées.

La transparence est cruciale, tant en interne qu'en externe. En interne, vous devez avoir une idée claire de tous les traitements de données à caractère personnel sous la responsabilité de votre organisation et vous devez sensibiliser le personnel à ce sujet. En externe, vous devez informer plus clairement les personnes dont vous traitez les données quant à leurs droits, à la manière dont elles peuvent exercer ces droits et aux tenants et aboutissants de l'activité de traitement.

2ère ÉTAPE : TENIR UN REGISTRE DES ACTIVITÉS DE TRAITEMENT

Bien que la tenue d'un registre de traitement ne soit pas une obligation pour les organisations comptant moins de 250 employés, il s'agit d'un bon outil pour faire le point et il est vivement recommandé pour toutes les organisations par la Commission de la protection de la vie privée.

Notez qu'une organisation de moins de 250 employés devra tout de même tenir un registre de traitement si (voir pages 15 et 16 du vade-mecum pour les PME) :

- Le traitement de données à caractère personnel n'est pas occasionnel (c'est-à-dire quasiment toutes les sociétés notamment dans le cadre de la gestion de leur personnel) ; ou
- le traitement comporte un risque pour les droits et libertés des personnes concernées; ou
- le traitement concerne des données sensibles.

Pour résumer : Une organisation de moins de 250 personnes peut limiter l'objet de son registre à ses traitements habituels de données, comme la gestion des salaires et du personnel. Les traitements occasionnels de données peuvent ne pas figurer dans le registre à moins qu'il ne s'agisse de traitements à risque pour les droits et libertés des personnes concernées ou de traitements de données sensibles au sens large.

Effectuer cet inventaire des données à caractère personnel que vous conservez vous permettra de voir plus clair afin de décider quelles actions mener. De plus, vous pourrez identifier et évaluer plus aisément les risques liés aux différents traitements.

- *Un exemple de registre traitement* (document Excel à télécharger) se trouve sur le site de la Commission de la protection de la vie privée. Pas de panique, il ne doit pas être rigoureusement complété, il s'agit de votre document de travail personnel : mettez-y les informations qui vous semblent nécessaires et dont vous avez connaissance. Les données à caractère personnel ne doivent pas être reprises directement dans ce tableau, indiquez plutôt des catégories (ex. données relatives au personnel : Nom, prénom, coordonnées, numéro de compte bancaire, etc. ; listing X : Nom, prénom, adresse, etc. ; carnet d'adresses : … , etc.)

Voici un exemple de fiche complétée pour vous aiguiller :

Modèle de fiche à porter au registre (Belgique)	
Processus opérationnel/traitement	Newsletter « InfoPro »
Description fonctionnelle du traitement	Service d'informations non-commercial Fondement : Consentement des abonnés
Données utilisées et personnes concernées	Nom, prénom, adresse e-mail des abonnés
Sous-traitant	Mailchimp
Échange de données	Non
Technologie	Logiciel d'email marketing de Mailchimp
Risque et mesure de sécurité	Risque : Fuite de données – Mesures de sécurité : Vérification de la conformité de Mailchimp au regard du RGPD OK + mots de passe
Droits des personnes concernées	Voir Charte vie privée de CPW
Statut	Continu (Durant le temps nécessaire pour atteindre la finalité)
Remarque(s)	Mise en conformité avec le RGPD effectuée le … suite à la demande de consentement des membres de la liste d'envoi.

- Voici un autre exemple de fiche de traitement à porter à votre registre selon le modèle proposé par la Commission Nationale de l'Informatique et des Libertés (CNIL), qui est l'Autorité de protection des données française :

Modèle de fiche à porter au registre (France)	
Traitement n°1	Newsletter « InfoPro »
Nom et adresse du responsable du traitement :	Culture Point Wapi Rue de la Citadelle n°124 / bte 29 7500 Tournai
Date de mise en oeuvre :	04 mai 2018
Finalité principale :	Communication - Informations à destination des acteurs culturels et autres partenaires de l'agence
Détail des finalités du traitement	- Envoi d'informations sur l'actualité culturelle de Wallonie picarde - Communication sur les fiches qui ont récemment été modifiées sur le site de l'agence
Service chargé de la mise en oeuvre	Service communication de l'agence
Fonction de la personne auprès duquel s'exerce le droit d'accès	Chargée de communication de l'agence

Catégorie de personnes concernées par le traitement	- Partenaires - Acteurs culturels de Wallonie picarde - Membres de l'assemblée générale - Personnes abonnées à la newsletter, - …	
Données traitées	Catégories de données traitées	Détails des données traitées
	Données d'identification	- Nom et prénom - Adresse email
Catégories de destinataires	Catégorie de destinataires	Données concernées
	Chargée de communication de l'agence	Toutes
Durée de conservation	Durant le temps nécessaire pour atteindre la finalité : Les données sont conservées tant que perdure l'Infopro et seront supprimées si Culture point wapi n'y a plus recours.	
Mise à jour (date et objet) :	Liste mise à jour le …. suite à la demande de consentement des membres de la liste d'envoi (mise en conformité avec le RGPD)	

QUELQUES POINTS D'ÉCLAIRCISSEMENTS POUR COMPLÉTER LE REGISTRE

a. Base juridique

Pour être légitime, chaque traitement de données à caractère personnel doit reposer sur une des bases juridiques énumérées à l'article 6 du RGPD. Le RGPD distingue six bases juridiques différentes (voir pp. 8 à 10 du vade-mecum pour les PME) :

1. Le consentement
2. Le contrat
3. Le respect d'une obligation légale
4. La sauvegarde d'un intérêt vital
5. L'exécution d'une mission d'intérêt public
6. L'intérêt légitime poursuivi par le responsable du traitement ou par un tiers

- Vos traitements reposeront principalement sur les fondements suivants :
  - **Consentement** - ex. Les personnes ont explicitement consenti à ce que je leur envoie ma newsletter. – cfr infra
  - **Contrat** - ex. je traite les données de mes employés dans le cadre de l'exécution de leur contrat de travail.
  - **Respect d'une obligation légale** - ex. Je suis légalement tenu de conserver telles données pendant X années.
  - **Intérêt légitime** - ex. Il est dans mon intérêt de conserver ces données pour assurer le bon fonctionnement de mon organisation. Attention, l'intérêt légitime à utiliser les données ne doit pas être (trop) préjudiciable pour la personne concernée. Cette mise en balance des intérêts doit se faire avec beaucoup de précaution.

b. Principe de finalité

Le principe de finalité est un fondement crucial du RGPD. Selon l'article 5.1.b) du RGPD, vous ne pouvez traiter des données à caractère personnel que pour des finalités qui ont été définies explicitement au préalable. En principe - mais il existe des exceptions -, il est interdit de traiter ultérieurement les données obtenues pour une autre finalité qui n'était pas prévue initialement. Il s'agit du principe de base.

Trois possibilités se présentent si vous souhaitez quand même traiter des données à caractère personnel pour une finalité qui diverge de celle pour laquelle vous avez initialement traité ces données :

1. Consentement distinct
2. Obligation légale
3. Compatibilité

Ces trois possibilités sont décrites en détail aux pages 10 et 11 du vade-mecum pour les PME.

c. Principes d'exactitude et de qualité des données et délai de conservation

Les données en votre possession doivent être exactes et à jour - p. 11 vade-mecum

De plus, vous ne pouvez conserver les données que pendant le délai nécessaire à la réalisation des finalités engagées. Ex. À la fin d'un projet pour lequel vous avez recueilli des données à caractère personnel, vous êtes supposés supprimer celles-ci (ex. listings des participants, etc.) Pour autant, bien entendu, que vous ne soyez pas tenus légalement de les garder pendant une certaine durée (archives, etc.)

d. Sous-traitants

Il s'agit des prestataires de services externes auxquels vous avez recours.
(Ex. MailChimp, OVH, Google, votre service cloud, etc.) Vous devez vous assurer que ceux-ci offrent les garanties nécessaires en matière de protection des données. Ces informations sont le plus souvent disponibles sur leur site internet. Si vous travaillez avec des prestataires sérieux, il y a de grandes chances que ce soit le cas.

3ère ÉTAPE : DÉSIGNATION D'UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Toutes les institutions ne devront pas désigner un délégué à la protection des données. La désignation est obligatoire dans trois cas :

- Une autorité publique effectue le traitement ; ou
- les activités de base de l'organisation consistent en une observation à grande échelle et systématique des personnes concernées ; ou
- les activités de base de l'organisation consistent en un traitement à grande échelle de données sensibles.

Cette exigence n'étant probablement pas une obligation pour votre structure, nous ne nous y arrêterons pas davantage. Pour plus d'informations, veuillez consulter les pages 16 et 17 du vade-mecum pour les PME.

- Notez cependant qu'il peut être intéressant de désigner une personne chargée de l'aspect « protection des données » au sein de votre institution.

4ère ÉTAPE : CAS PRATIQUE - LES NEWSLETTERS

En principe, vous devez dorénavant vous assurer que les destinataires de votre newsletter aient consenti à recevoir celle-ci.

Une mention permettant aux destinataires de se désabonner ne suffit plus. Si vous souhaitez être en parfaite conformité avec le RGPD, vous devrez contacter l'ensemble des destinataires de votre newsletter et leur demander s'ils acceptent d'être abonnés à celle-ci (bouton oui/non). Vous ne pourrez alors conserver dans votre liste d'envoi que les adresses e-mail de personnes ayant donné leur accord. C'est ce qu'on appelle l'opt-in, contrairement à l'opt-out qui était la tendance jusqu'à présent. On considère même qu'un double opt-in serait aujourd'hui nécessaire.

C'est-à-dire que la personne qui clique sur le bouton « Oui, je consens à recevoir votre newsletter » devrait ensuite recevoir un e-mail de confirmation avec un lien cliquable qui vient confirmer son consentement. Cette exigence s'applique surtout pour les newsletters à caractère commercial et il n'est peut-être pas nécessaire d'en arriver là à notre échelle, qui plus est dans le secteur non-marchand pour des newsletters purement informatives.

- **Attention, vous devez être en mesure d'apporter la preuve du consentement des individus.** Ainsi, dans le cadre de votre infolettre, vous devez donc être en mesure de fournir la preuve du consentement des destinataires. Vous devez donc avoir en votre possession: les données de l'individu, la date d'obtention des données, son accord pour recevoir votre infolettre ; un courriel de confirmation (si double opt-in).

- **Comment gérer le désabonnement des newsletters ?** Un processus de désabonnement simple, clair et efficace doit systématiquement être présent dans chacune de vos newsletters. L'idéal est d'associer à ce processus la possibilité de contacter une adresse courriel de retour.

- **L'opt-out & opt-in passif désormais interdits**
  - **Opt-out** : pratique consistant à inscrire d'office un utilisateur à une liste après une inscription à un service, en lui laissant la charge de se désinscrire.
  - **Opt-in passif** : pratique consistant à obtenir le consentement d'un internaute de manière détournée, le plus souvent en pré-cochant la case correspondant au souhait de recevoir des emails de la part de l'entreprise.
  - **Opt-in** : pratique consistant à laisser l'internaute exprimer librement son consentement par une action positive, généralement en cochant de lui-même une case correspondant au souhait de recevoir des emails de votre part.

Au vu de cette nouvelle définition du consentement, il sera désormais strictement interdit d'utiliser des adresses emails obtenues par opt-out ou par opt-in passif. Le consentement devra être demandé de manière explicite via la méthode de l'opt-in uniquement. Seules les listes 100% opt-in seront utilisables légalement.

A vous de faire votre choix entre ces formules, le risque étant de perdre un grand nombre de vos abonnés si vous respectez la réglementation à la lettre.
Mais ne faut-il pas mieux parfois miser sur la qualité que sur la quantité ? :-)

5ère ÉTAPE : DROITS DE LA PERSONNE CONCERNÉE (VOIR P.21 ET S. DU VADE-MECUM)

Vérifiez si les procédures actuelles dans votre 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.
Outre l'imposition de certaines obligations qui ont été abordées ci-dessus, le RGPD prévoit des droits que chaque personne concernée peut exercer. La personne concernée exerce ces droits à l'égard du responsable du traitement. Le sous-traitant doit assister le responsable du traitement pour permettre l'exercice de ces droits. Il s'agit en particulier des :

1. Droit à l'information/de l'obligation d'informer
2. Droit d'accès
3. Droit de rectification
4. Droit à l'effacement des données
5. Droit à la limitation du traitement des données
6. Droit d'opposition
7. Droit à la portabilité des données
8. Droit de ne pas faire l'objet d'une décision individuelle automatisée.

6ère ÉTAPE : SÉCURITÉ

Il est intéressant d'avoir une réflexion sur les mesures techniques et organisationnelles mises en place pour garantir la protection des données à caractère personnel (par ex. contre un accès ou un traitement non-autorisés, la perte, les dégâts, le vol) et décider de mettre certaines mesures en place. Les mesures à mettre en place dépendent fortement de l'importance du risque et des menaces. Vous trouverez plus d'information aux pages 13 et suivantes du vade-mecum pour les PME.

Quelques pistes à explorer pour assurer la sécurité des données en votre possession :

- Sensibilisation et formation ; Politique de mots de passe ; Antivirus ; Mises à jour ; Sites sécurisés/https ; Sauvegarde/back-up ; Chiffrement ; Sécurité des locaux ; …

En cas de violation des données, il existe 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. Cette exigence ne s'applique que lorsque la violation en question est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. La situation est à évaluer au cas par cas. (Ex. une photo prise à la fête du personnel est publiée, il n'y aura pas d'impact et cela ne devra pas être déclaré. Par contre une donnée judiciaire (qui est une donnée sensible), comme le certificat de bonne vie et mœurs, c'est autre chose.)