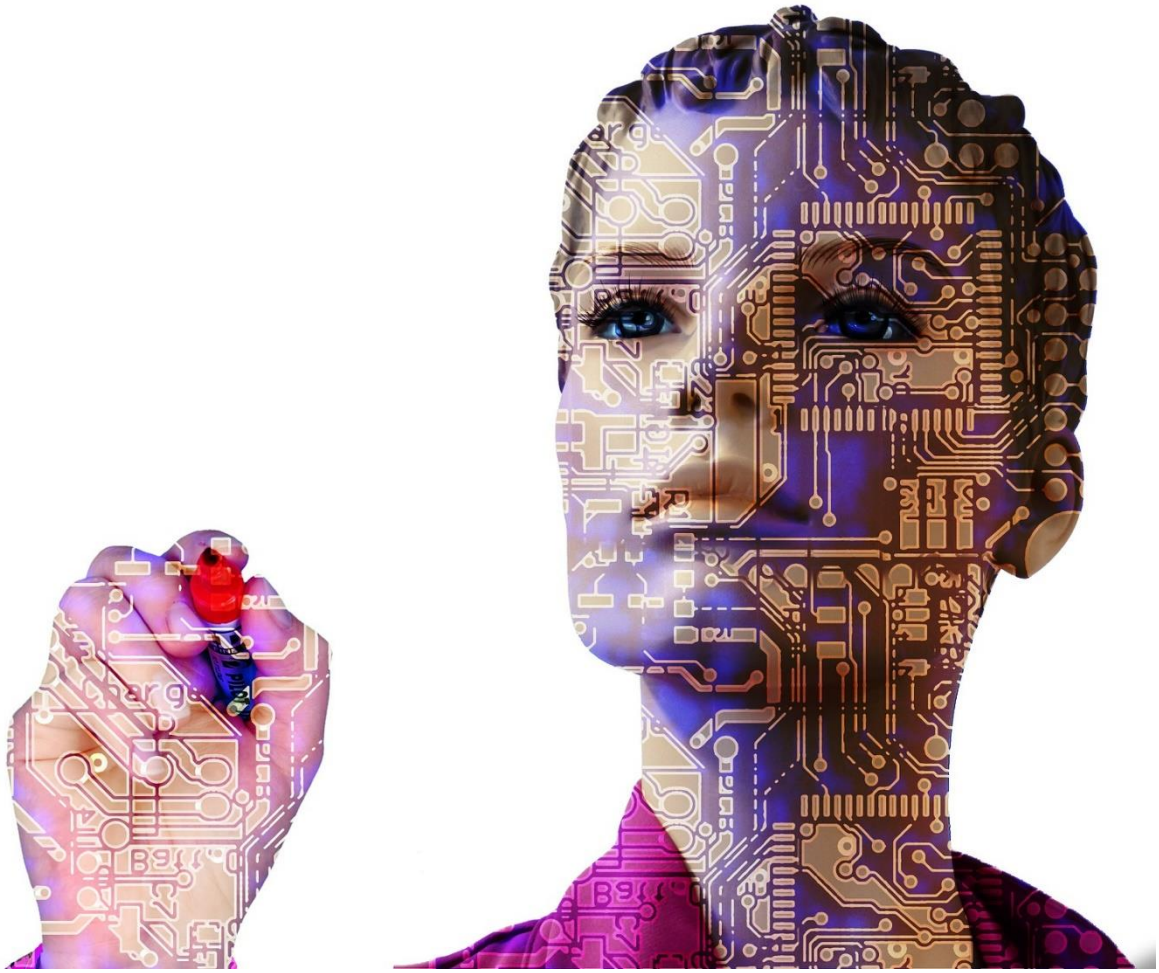
BE LARP

LE RGPD EN GN



INTENTION

Suite à la remise sur le devant de la scène de la thématique de la protection de la vie privée par l'introduction du **Règlement Général sur la Protection des Données. (RGPD), nous voulons vous informer simplement des implications concrètes de celui-ci dans le cadre de vos activités et rappeler quelques éléments de base concernant la gestion de données.**

Ce document ne se veut pas exhaustif et passera certains points dans un souci de simplicité. De nombreux documents (dont le texte complet du règlement) sont disponibles en ligne.

Afin de ne pas réinventer la roue, ce document se base sur d'autres synthèses provenant de :

- **La FESOJ**
- **La CNIL**
- **Le CJC**
- **La Mutualité Chrétienne / Jeunesse et Santé / ALtéo / Enéo**
- **La CPVP**
- **Le Cabinet CustUp**

Une « petite » ASBL ou association de fait est elle sujet au RGPD ?

OUI

La loi ne s'applique pas dans le cadre d'activités exclusivement personnelles ou domestiques, comme la tenue d'un fichier d'adresses privé ou d'un agenda personnel électronique.

DÉFINITION

Le GDPR entrera en vigueur le 25 mai 2018 et remplacera certaines directives publiées dans les années 1990. Il est évident que depuis le milieu des années 1990, le paysage technologique et numérique a beaucoup évolué. La RGPD a été conçue pour **adapter et moderniser le cadre juridique** en matière de protection des données à ces évolutions.

Plus largement, la RGPD a pour ambition de **« redonner aux citoyens le contrôle de leurs données personnelles ».**

DÉONTOLOGIE ET SECRET DES DONNÉES

Outre le RGPD, il est important de resituer un article du code pénal s'appliquant à toutes les organisations de GN.

Globalement, l'équipe organisatrice et les bénévoles ont accès, pour une bonne organisation, à des informations et données de différents types. Celles-ci peuvent être plus ou moins sensibles selon les cas. Les personnes détentrices de ces informations restent pénalement responsables des secrets (**TO et TI**) pour lesquels s'applique l'article 458 du code pénal.

> *Art. 458 Code pénal*
> *Les médecins, chirurgiens, officiers de santé, pharmaciens, sages-femmes et toutes autres personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où ils sont appelés à rendre témoignage en justice ou devant une commission d'enquête parlementaire et celui où la loi les oblige à faire connaître ces secrets, les auront révélés, seront punis d'un emprisonnement de huit jours à six mois et d'une amende de cent euros à cinq cents euros.*

CHAMPS D'ACTION

Les règles et obligations du GDPR s'appliquent au traitement – automatisé ou non – des données à caractère personnel.

- **Donnée à caractère personnel (DCP)** : toute information se rapportant à une personne physique identifiée ou identifiable ».
  Par personne physique identifiable, il faut comprendre « une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».
- **Traitement des données** : fait référence à la **collecte**, à l'**accès**, au **stockage**, à la **manipulation**, à la **destruction** et à la **consultation à distance** des données.
  Concrètement, une entreprise qui délègue à un prestataire la collecte et le stockage des données fait néanmoins du traitement de données dans la mesure où elle les consulte.

LES 4 PRINCIPES CLÉS

CONSENTEMENT ET TRANSPARENCE

Le consentement des individu.e.s quant à la collecte et au traitement des données à caractère personnel les concernant devra être explicite et « positif ». Ce consentement pourra être retiré à tout moment par les individus le demandant.

> *Consentement de la personne concernée*
> *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*

La transparence est le deuxième grand principe mis en avant par la RGPD. Il s'articule au consentement, dans la mesure où la transparence est la condition de possibilité d'un **consentement explicite et éclairé.**

Les entreprises devront – et ce dès la phase de collecte – fournir aux individu.e.s des informations claires et sans ambiguïté sur **la manière dont leurs données seront traitées.**

Ces informations devront être fournies de façon concise, compréhensive et accessible par tous (par exemple, sur les formulaires de collecte, dans les documents contractuels, sur la page du site relative à la politique de « privacy », etc.).

TRAITEMENT LICITE

Le traitement de données à caractère personnel ne sera licite que :

- Si la personne concernée a donné son consentement ;
- Si le traitement est nécessaire à l'exécution d'un contrat ;
- Si le traitement est exigé par une loi, un décret ou une ordonnance ;
- Si le traitement est nécessaire pour sauvegarder un intérêt vital ;
- Si le traitement est nécessaire pour exécuter une mission d'intérêt public ;
- Si le traitement est nécessaire pour réaliser un intérêt légitime du responsable.

TRAITEMENT LOYAL ET TRANSPARENT, COLLECTE À DES FINS DÉTERMINÉES

Celui ou celle qui collecte les données **doit indiquer pourquoi il/elle veut obtenir ces données**. Cette personne ne peut faire croire qu'il poursuit un but alors qu'il a l'intention de faire autre chose avec les données collectées.

Cette personne ne peut pas non plus agir à l'insu des personnes, elles doivent être informées de la manière dont leurs données seront utilisées.

DONNÉES COLLECTÉES ADÉQUATES ET PERTINENTES.

Le **but de la collecte doit bien être spécifié** et les données demandées pertinentes au vu de cet objectif.

Par exemple, si on souhaite établir un fichier d'adresses pour l'envoi d'une newsletter, l'adresse mail sera pertinente mais pas une date de naissance ou un état civil.

DONNÉES SENSIBLES

En principe, on n'a pas le droit de collecter certaines données dites sensibles, à savoir les données relatives :

- à l'ethnie
- aux opinions politiques
- aux convictions religieuses et philosophiques
- à l'appartenance syndicale
- **à la santé**
- à la vie sexuelle
- à des suspicions, des poursuites ou des condamnations pénales ou administratives.

Toutefois, des exceptions sont admises si les personnes ont donné leur consentement explicite ou dans le cadre de soins de santé ou de recherche scientifique.

DONNÉES EXACTES ET TENUES À JOUR

Le responsable du traitement doit veiller à ce que les données soient exactes et mises à jour si nécessaire. Il doit également prendre les mesures nécessaires pour corriger ou effacer les données inexactes ou incomplètes.

DURÉE DE CONSERVATION DES DONNÉES

Les données personnelles ne doivent pas être conservées plus longtemps qu'il n'est nécessaire par rapport à l'objectif poursuivi. Il conviendra alors de les effacer ou de les rendre anonymes.

SÉCURITÉ DES TRAITEMENTS & CONFIDENTIALITÉ

Le responsable du traitement doit veiller à ce que les personnes travaillant sous son autorité ne puissent avoir accès qu'aux données dont elles ont besoin pour exercer leurs fonctions.

Il est aussi important de protéger les données contre une curiosité malsaine (interne ou externe) et contre des manipulations non autorisées.

DROIT DES PERSONNES

DROIT À L'INFORMATION

A partir du moment où l'on recueille des données sur des personnes, on doit informer ces personnes de ce que l'on compte en faire. On ne peut pas traiter de données à l'insu des sujets.

DROIT À LA CURIOSITÉ

Chacun.e a le droit d'interroger tout responsable de traitement pour savoir s'il détient ou non des données le concernant. Le ou la responsable doit alors confirmer ou non s'il détient des données, et si c'est le cas, préciser dans quel but, de quelles catégories de données et quels en sont les destinataires.

DROIT D' ACCÈS

Chacun.e a le droit de recevoir, sous une forme intelligible, une copie des données faisant l'objet d'un traitement ainsi que toute information sur l'origine des données. Ce droit est exerçable par demande au responsable de traitement en faisant la preuve de son identité, par tout moyen de communication.

DROIT DE RECTIFICATION

Toute personne peut faire rectifier des données inexactes qui se rapportent à lui, ou faire effacer ou interdire l'utilisation de données incomplètes ou non pertinentes (et ce sans aucun frais).

DROIT D'OPPOSITION

Chacun.e peut s'opposer au traitement de ses données mais en invoquant des raisons sérieuses et légitimes. Dans le cas de marketing direct, l'opposition sera gratuite et sans aucune justification nécessaire.

DROIT DE NE PAS ÊTRE SOUMIS À UNE DÉCISION AUTOMATISÉE

La loi interdit qu'une décision affectant une personne de manière significative soit prise sur le seul fondement d'un traitement automatisé. Cette interdiction ne s'applique pas si le traitement est fondé dans le cadre d'un contrat ou d'une disposition légale ou réglementaire.

RESPONSABILITÉS

MESURES TECHNIQUES ET ORGANISATIONNELLES - - POLITIQUE DE PROTECTION DES DONNÉES

- Les mesures de sécurité à mettre en œuvre sont de deux ordres : des mesures organisationnelles (limite le nombre de personnes ayant accès aux données, utilisation de mots de passe, locaux fermés,
- etc.) et des mesures techniques (anonymisation des données, chiffrement et encryptage, etc.).

ETABLIR UN REGISTRE DES ACTIVITÉS DE TRAITEMENT

La loi prévoit une obligation de déclaration des traitements de données. Toutefois, les traitements suivants sont exemptés de déclaration :

- Traitement réalisé par une société pour la gestion du personnel
- Traitement réalisé par une fondation ou ASBL concernant ses membres, bienfaiteurs.trices et contacts réguliers
- Traitement réalisé par les écoles et les établissements d'enseignement concernant leurs élèves et étudiant.e.s

Cependant, malgré la dispense de déclaration, le.la responsable de traitement doit tenir à la disposition de toute personne qui en fait la demande un registre des activités de traitement qui reprend :

- La dénomination du traitement
- La finalité ou les objectifs
- Les catégories de données traitées
- Les bases légales ou réglementaires
- Les destinataires à qui les données peuvent être fournies
- Les garanties entourant la communication de données à des tiers
- Les moyens d'information aux personnes dont les données sont traitées
- Les coordonnées d'un.e responsable auprès duquel les personnes concernées pourront exercer leurs droits
- Les catégories de données transmises à l'étranger, le pays de destination et les raisons permettant le transfert
- La période de validité des données
- Les mesures organisationnelles et techniques de sécurité

OBLIGATION DE SIGNALER UNE VIOLATION OU FUITE DE DONNÉES

En cas de violation de données ou de fuite de données, le responsable du traitement doit informer l'autorité de contrôle dont il dépend de la violation ou fuite et ce dans les 72 heures. Il existe une exception si la violation ou fuite ne représente pas de risque pour les droits et libertés des personnes concernées. Par ailleurs, si un tel risque existe, le.la responsable de traitement doit également informer les personnes concernées par cette violation ou fuite.

CONCRÈTEMENT

Dans le monde du GN certaines pratiques (déjà condamnables par le passé) ne peuvent plus exister ou être adaptées en conséquence de GRPD

- La mise en place de listing public de nom et prénom des participants (incluant parfois le statut du paiement) sur un site web ou sur Facebook (groupe, event,…)
- L'utilisation de consentement implicite ou négatif (case à cocher : je ne souhaite pas…ou consentement tacite)
    - L'ajout automatique des mails des participants dans un listing de newsletter
    - La prise de photographie sans consentement
- Le recueil des numéros de registre national (formellement interdit sans autorisation de l'état)

Une des craintes formulées face à cette réglementation est l'opposition (systématique) de joueurs et joueuses face à la politique de traitement de données. En effet, en invitant les participants et participantes à approuver la politique de traitement vous vous exposer à des oppositions de principe.

Heureusement, dans la majeure partie des cas, la relation orga-participant.e rentre dans le cadre de « nécessité à l'exécution du contrat » et de la « sauvegarde d'un intérêt vital » (pour les données médicales)

Bien qu'une personne puisse, en théorie s'opposer au traitement de ses données médicales, en cas d'accident, sa responsabilité sera engagée pour ne pas vous avoir communiquer des informations capitales relatives à sa santé

En définitive, il est primordial d'informer sur les modalités de traitement telle que le prévoir le RGPD mais le refus du traitement des données nécessaires à la bonne exécution de l'activité peut être une close de nullité. En l'état, vous pourriez exiger l'acceptation de la politique de confidentialité selon vos propres termes.

KEEP IN MIND

TEMPLATE DE POLITIQUE DE CONFIDENTIALITÉ

A Venir

EXEMPLE

Cet exemple est repris du site d'un de nos membres et utilisé dans le cadre de l'inscription (de faction) à AVATAR. **http://reve-emotion.be/index.php/events/marble-black-2018/**

Politique de traitement des données personnelles

Vos données personnelles ne seront accessibles qu'aux membres organisateurs affiliés à Rêve-Emotion ASBL.

- Votre adresse mail servira de moyen de contact privilégié avec l'organisation pour la bonne préparation de l'évènement.
- Une case supplémentaire peut être cochée pour marquer votre accord explicite d'être tenu informé de nos activités en dehors de la faction de Marble Black.
- La date de naissance des participants nous permet d'être au courant de la présence d'enfants et de mineurs au sein de la faction.
- Le numéro de GSM nous servira à vous contacter en cas d'urgence ou si un mail ne s'avérait pas adapté.
- Vos intolérances ou régime alimentaire particulier, dans le cas d'une inscription à l'intendance, seront communiqués à l'équipe cuisine afin de prévoir un menu adapté.
- Vos remarques médicales, si vous jugez utile de nous en informer, nous permettront de réagir de façon adaptée en cas d'urgence et de tenir le responsable médical informé.
- Les photos prise par un photographe de la faction (différent des photographes AVATAR) ne seront pas publiées sur facebook et ne seront utilisées qu'à des fins de promotion des activités de l'ASBL (disponibles dans une galerie sur le site web).