
GRATUiT
MATINÉE D'INFORMATIONS
RGPD
JEUDI 03\05\2018 > 9:00
LIÈGE \ CITÉ MIROIR
ethias
FÉDÉRATIONS ET CLUBS SPORTIFS
VOS NOUVELLES OBLIGATIONS POUR LA PROTECTION GÉNÉRALE DE VOS DONNÉES
AISF
Association Interfédérale du Sport Francophone

Règlement Général sur la Protection des Données (RGPD) - Contextualisation

Mardi 23
Parlement
Règles

AISF Association Interfédérale du Sport Francophone

Pourquoi une nouvelle règlementation?

<u>Cadre actuel</u>:

Directive UE 95/46 -> Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

- ► cadre dépassé
- ► nécessité d'un cadre unifié

AISF Association Interfédérale du Sport Francophone

Principes de base

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 » *(article 4 RGPD)*

Principes de base

DONNEES A CARACTERE PERSONNEL

« Toute information se rapportant à une personne physique identifiée ou identifiable [...]. » *(article 4 RGPD)*

Principes de bases

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 [...]. » *(article 4 RGPD)*

Principes de base

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. » *(article 4 RGPD)*

Principes généraux

- ✓ Licéité, loyauté, transparence
- ✓ Limitation des finalités
- ✓ Minimisation des données
- ✓ Exactitude
- ✓ Limitation de la conservation
- ✓ Intégrité & confidentialité

AISF Association Interfédérale du Sport Francophone

Merci pour votre attention !

Mardi 21 octobre 2014
Parlement de la Fédération Wallonie-Bruxelles

AISF Association Interfédérale du Sport Francophone

Les associations face au Règlement Général de Protection des Données (GDPR)

Dominique Counasse

Liège – 3 mai 2018


ON YOUR MARK
GET READY
ANY TIME NOW
REALLY SOON...
GDPR

1 – QU'EST-CE QUE LE GDPR ?

- **Règlement 2016/679 du Parlement européen et du Conseil**
- **adopté le 27 avril 2016,**
- **entrant en vigueur le 25 mai 2018,**
- **d'application immédiate sans nécessité d'une transcription en droit belge,**
- **précisant et élargissant les principes déjà énoncés par une directive précédente transposée en droit belge par la loi du 8/12/92.**
- **Des Guidelines établies par le Working Party 29 (futur Comité européen de la protection des données).**
- **Une loi belge en préparation pour préciser les mesures de portée nationale (infractions pénales, mesures de protection complémentaires, autorité de contrôle,…).**

2 – QUE VISE LE GDPR ?

- Un **traitement**
- de **données personnelles,**
- dont certaines – les **données sensibles** – doivent être particulièrement protégées,
- données se rapportant à des personnes (les **personnes concernées**) dont il importe de sauvegarder les intérêts,
- traitement effectué par un **responsable du traitement**
- qui peut déléguer ce traitement à un **sous-traitant**
- ou qui peut transmettre les données en question à un **destinataire,**
- étant entendu que tout **transfert de données hors EEE** est sévèrement contrôlé et limité.

3 – QUELS PRINCIPES ÉNONCE-T-IL ?

Les données personnelles doivent être

- **traitées de manière légale, transparente et que leur utilisation soit facile à comprendre pour la personne concernée,**
- **pertinentes et limitées à l'objectif poursuivi,**
- **collectées dans un but déterminé, explicite et légal,**
- **exactes et tenues à jour,**
- **conservées uniquement durant le délai nécessaire au traitement poursuivi,**
- **et traitées en prenant des mesures de sécurité informatique adéquates.**

4 – QUEL TYPE DE TRAITEMENT EST VISÉ ?

- **Traitement de données à caractère personnel.**
- **Automatisé en tout ou en partie.**
- **Non automatisé de données contenues ou appelées à figurer dans un fichier (ensemble structuré de données centralisé ou non et accessible selon des critères déterminés).**

➔ **Applicable**

- **à des données structurées (figurant dans des champs informatiques),**
- **à des données non structurées (mails, documents scannés, …).**

5 – UNE ASSOCIATION EFFECTUE-T-ELLE UN TRAITEMENT DE DONNÉES ?

La définition du traitement de données est fort large :

Opération ou ensemble d'opérations appliquées à des données personnelles ou à un ensemble de données personnelles telles que

- **Collecte,**
- **Enregistrement,**
- **Conservation,**
- **Extraction,**
- **Consultation,**
- **Utilisation,**
- **Communication par transmission,**
- **Diffusion,**
- **Interconnexion,**
- **Modification,**
- **Effacement ou destruction.**

➔ **La réponse est Oui**

6 – QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

- Toute information concernant une personne physique identifiée ou identifiable vivante.
- Données d'identification: Nom, NISS, adresse postale, numéro de compte bancaire, adresse mail, adresse IP, …
- Données professionnelles et privées associées à cet identifiant.
- Données sensibles :
  - données génétiques ou biométriques,
  - données relatives à la santé,
  - à l'origine raciale ou ethnique,
  - aux opinions politiques, aux convictions philosophiques ou religieuses, à l'appartenance syndicale,
  - à la vie ou à l'orientation sexuelle.

7 – UNE ASSOCIATION TRAITE-T-ELLE DES DONNÉES PERSONNELLES ?

Généralement toute affiliation à une association implique la collecte et l'utilisation de données telles que

- les coordonnées d'une personne (nom, prénom, adresse),
- son numéro de compte bancaire (domiciliation bancaire),
- son adresse mail (pour permettre la communication),
- des informations concernant sa famille (si on les affilie également et parfois avec des tarifs réduits).

➔ La réponse est **Oui**

8 – UNE ASSOCIATION TRAITE-T-ELLE DES DONNÉES SENSIBLES ?

De par leur nature, certaines associations traitent effectivement des données sensibles :

- **Eglises, Cultes**
- **Loges maçonniques**
- **Syndicats**
- **Associations de victimes**
- **Associations de patients, d'handicapés ou de malades chroniques**
- **Associations de défense ou de promotion culturelle**
- **Associations de défense contre la discrimination**
- **…**

9 – UN CERTIFICAT D'APTITUDE AU SPORT EST-IL UNE DONNÉE DE SANTÉ ?

Il est rédigé par un médecin ➔ il constitue bien une donnée relative à la santé physique d'une personne !

IL FAUT DONC ÊTRE EXTRÊMEMENT ATTENTIF

- **à son contenu : mentionne-t-il uniquement l'aptitude à la pratique d'un sport en particulier ou de tout sport en général ? Fait-il état d'une pathologie handicapante ?**
- **à son mode de transmission (pli fermé ou non)**
- **à son destinataire, à savoir celui qui en demande la production et qui le conserve (l'association pour protéger sa responsabilité éventuelle ou l'assureur pour voir s'il va assurer ou non l'affilié)**

CAR LES RESPONSABILITES ET LES SECURITES VARIENT EN CONSEQUENCE

10 – QUELLES PERSONNES SONT PROTÉGÉES PAR LE GDPR ?

- Personnes physiques vivantes.
- Avec une protection particulière pour les enfants (personnes âgées de moins de 16 ans avec une possibilité pour les Etats membres de porter cet âge à 13 ans).
- Pas les personnes morales.
- Mais bien leurs représentants.
- Pas les personnes physiques décédées.

11 – QUELLES SONT LES PERSONNES DONT UNE ASSOCIATION POSSÈDE LES DONNÉES ?

On peut les classer en différentes catégories :

- **adhérents, membres,**
- **Sympathisants et donateurs,**
- **bénéficiaires d'une intervention,**
- **membres du personnel et représentants légaux de l'association**
- **fournisseurs,**
  - **personnes physiques,**
  - **représentants des personnes morales,**
- **intervenants divers (avocats, …),**

étant entendu que le type de données possédées varie en fonction de leurs catégories.

12 – QUELS SONT LES ACTEURS VISÉS PAR LE GDPR ?

L'article 4 du GDPR indique

- **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.**
- **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.**
- **Destinataire : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers (ce dernier étant placé sous l'autorité directe du responsable du traitement ou du sous-traitant).**

13 – EN PRATIQUE QUE FAIT LE RESPONSABLE DU TRAITEMENT ?

Il détermine les finalités (le pourquoi ?) et les moyens du traitement (le comment ?).

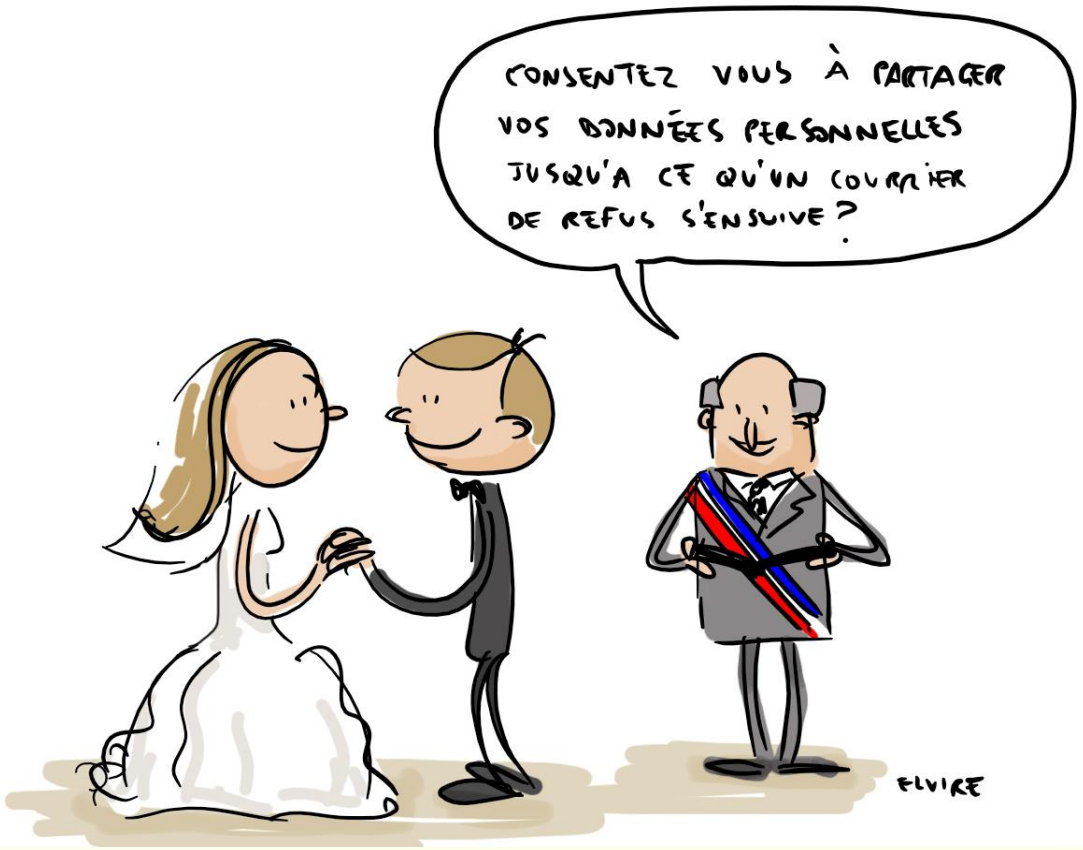
- **Il choisit les données à traiter et le type de traitement à appliquer.**
- **Il définit le mode de conservation des données et la durée de celle-ci.**
- **Il est garant de leur sécurité et définit donc les mesures applicables.**
- **Il choisit librement ses sous-traitants.**
- **Il doit en principe établir un registre de traitement des données.**

S'il fait cela de concert avec une autre personne physique ou morale on parlera alors de responsables conjoints.

14 – EN PRATIQUE QUE FAIT LE SOUS-TRAITANT ?

Il agit pour le compte du responsable du traitement.

- **Il ne peut traiter que les données prévues par le responsable et uniquement dans le cadre strictement prévu par ce dernier.**
- **Il doit appliquer les modes de conservation et la durée de conservation choisis par le responsable.**
- **Il doit mettre en œuvre les mesures de sécurité choisies par le responsable.**
- **Il doit faire agréer ses propres sous-traitants par le responsable.**
- **Il doit établir un registre des catégories de traitement effectuées pour le compte du responsable.**



www.ITisbeautiful.fr

15 – QUEL EST LE RÔLE D'UNE ASSOCIATION ?

Soit l'association traite les données pour son propre compte :

- **données des membres adhérents, des sympathisants donateurs,**
- **données de son personnel, de ses représentants légaux,**
- **données de ses fournisseurs,**
- **données collectées pour la réalisation de son objet social.**

➔Elle est alors le responsable du traitement

Soit l'association traite des données pour le compte de tiers :

- **parce qu'elle joue le rôle d'une centrale d'achats en vue de faire bénéficier ses membres de tarifs préférentiels,**
- **parce qu'elle collecte des données pour un assureur,**
- **parce qu'elle collecte des données pour une administration.**

➔ Elle est alors un sous-traitant

16 – UNE ASSOCIATION DE FAIT EST-ELLE VISÉE PAR LE GDPR ?

- Les personnes morales (ASBL, Fondations, Sociétés à finalité sociale, …) sont bien évidemment visées par le GDPR.
- Une association de fait, elle, n'a pas de personnalité juridique.
- Elle pose des actes par l'entremise des personnes physiques qui la représentent.
- Or les personnes physiques sont aussi visées par le GDPR et ne sont dispensées de son application que dans le cadre de leurs activités strictement personnelles ou domestiques, ce qui n'est pas le cas en l'espèce.

➔ Les personnes physiques qui la représentent doivent appliquer le GDPR

17 – QUEL EST LE RÔLE DES FOURNISSEURS DE L'ASSOCIATION ?

Il ne faut pas confondre un sous-traitant au sens du GDPR avec un fournisseur classique.

- **Certains fournisseurs sont bien des sous-traitants parce qu'ils traitent des données pour le compte de l'association. C'est le cas par exemple d'un secrétariat social ou d'un partenaire informatique hébergeant des données.**
- **Certains fournisseurs doivent être considérés comme des responsables de traitement notamment lorsqu'ils sont astreints de par la loi à collecter et gérer certaines données et même à les transférer à diverses autorités publiques (par exemple en matière pénale, fiscale et sociale ou de blanchiment). C'est le cas par exemple des banquiers, des opérateurs téléphoniques ou des sociétés de leasing automobile**

18 – QUEL EST LE RÔLE DE L'ASSUREUR ?

- **Un assureur est un responsable de traitement.**
  - Il détermine les données qu'il faut recueillir, analyser et conserver.
  - Il détermine la finalité et la base juridique du traitement des données.
- **Une association pourrait même être considérée comme son sous-traitant.**
  - Elle collecte les données des parties lésées (Assurances de responsabilité ou Accident corporel), des parties impliquées pour permettre un recours éventuel (Assurances de choses).
- **Le cas des assurances des membres du personnel.**
  - L'employeur traite les données dans le cadre de l'exécution de la relation professionnelle et afin de remplir ses obligations légales ➔ il est responsable du traitement.
  - Il les transmet ensuite à l'assureur afin de permettre à ce dernier d'honorer ses obligations contractuelles et, le cas échéant, de remplir ses obligations légales ➔ l'assureur est responsable d'un autre type de traitement.

19 – COMMENT SE CONFORMER AU GDPR ?

Il faut

- **identifier les données traitées,**
- **définir la base juridique de leur traitement,**
- **respecter les droits des personnes concernées,**
- **mettre en œuvre des mesures techniques et organisationnelles adéquates pour assurer la sécurité des données,**
- **prévenir l'autorité de contrôle en cas de violation de données à caractère personnel (Data breach).**

20 – UNE ASSOCIATION DOIT-ELLE TENIR UN REGISTRE DE TRAITEMENT?

En principe, tout responsable de traitement doit tenir un registre de traitement.

L'article 30 du GDPR dispense toutefois les entreprises et autres organisations comptant moins de 250 employés de tenir un registre de traitement des données sauf

- **si le traitement effectué porte sur des données sensibles,**
- **si le traitement effectué est susceptible de comporter un risque pour les droits et libertés des personnes concernées et n'est pas occasionnel.**

Dans la pratique, la plupart des associations seront donc dispensées de tenir un registre de traitement sauf celles traitant des données sensibles.

21 – UNE ASSOCIATION DOIT-ELLE DÉSIGNER UN DATA PROTECTION OFFICER (DPO) ?

L'article 37 du GDPR oblige les responsables de traitement et les sous-traitant à désigner un DPO

- en cas de traitement à grande échelle de données sensibles dont celles relatives à la santé,
- En cas de nécessité d'un suivi régulier et systématique des personnes concernées du fait de l'importance des traitements.

En pratique, la plupart des associations ne devront donc pas désigner de DPO.

Néanmoins, lorsqu'un DPO doit être désigné :

- il est le point de contact de l'autorité de contrôle,
- il contrôle la mise en œuvre et l'application des règles internes,
- il est impliqué dans les projets et les processus afin d'informer et de conseiller sur les respects des normes GDPR,
- il prend en charge le suivi des Data breach.

Un même DPO peut intervenir pour plusieurs associations !


I THINK THE NEW "DATA" PROTECTION OFFICER DOESN'T REALLY KNOW HIS OWN JOB...
HE SEEMS TO BE GUARDING THE "DATES" ...
CALENDER
LECTRR FOR CONTRAST

22 – QUELLE EST LA BASE JURIDIQUE DU TRAITEMENT DE DONNÉES ?

SOIT LE TRAITEMENT EST NÉCESSAIRE :

- à **l'exécution d'un contrat, en ce compris sa souscription**
  - **mais uniquement valable à l'égard du cocontractant,**
  - **Attention normes particulières pour les mineurs !**
- à **l'exécution d'obligations légales** à l'exécution d'une tâche effectuée dans **l'intérêt public** ou dans l'exercice de l'autorité publique confiée au responsable du traitement,
- dans **l'intérêt légitime** du responsable de traitement (ex. lutte contre la fraude, prospection en cas d'activité commerciale,…),

SOIT JE DOIS OBTENIR LE CONSENTEMENT DE LA PERSONNE CONCERNÉE.

LE TRAITEMENT DE DONNEES SENSIBLES, HORMIS EN DROIT SOCIAL, EST SUBORDONNE AU CONSENTEMENT EXPLICITE DE LA PERSONNE CONCERNEE.

23 – COMMENT GÉRER LE CONSENTEMENT ?

- **Le consentement exige une action affirmative claire.**
- **Le silence, les cases pré-cochées ou l'absence de réaction ne constituent pas un consentement !**
- **Le consentement doit être vérifiable. Cela signifie qu'il faut conserver une preuve concernant la façon et le moment où le consentement a été donné.**
- **Les individus ont le droit de retirer leur consentement à tout moment.**
- **On n'est pas tenu d'obtenir un nouveau consentement des personnes concernées si celui donné auparavant répond déjà aux nouvelles exigences. On doit donc s'assurer que ce dernier réponde bien aux normes requises par la nouvelle législation.**

23 – COMMENT GÉRER LE CONSENTEMENT ?

En pratique

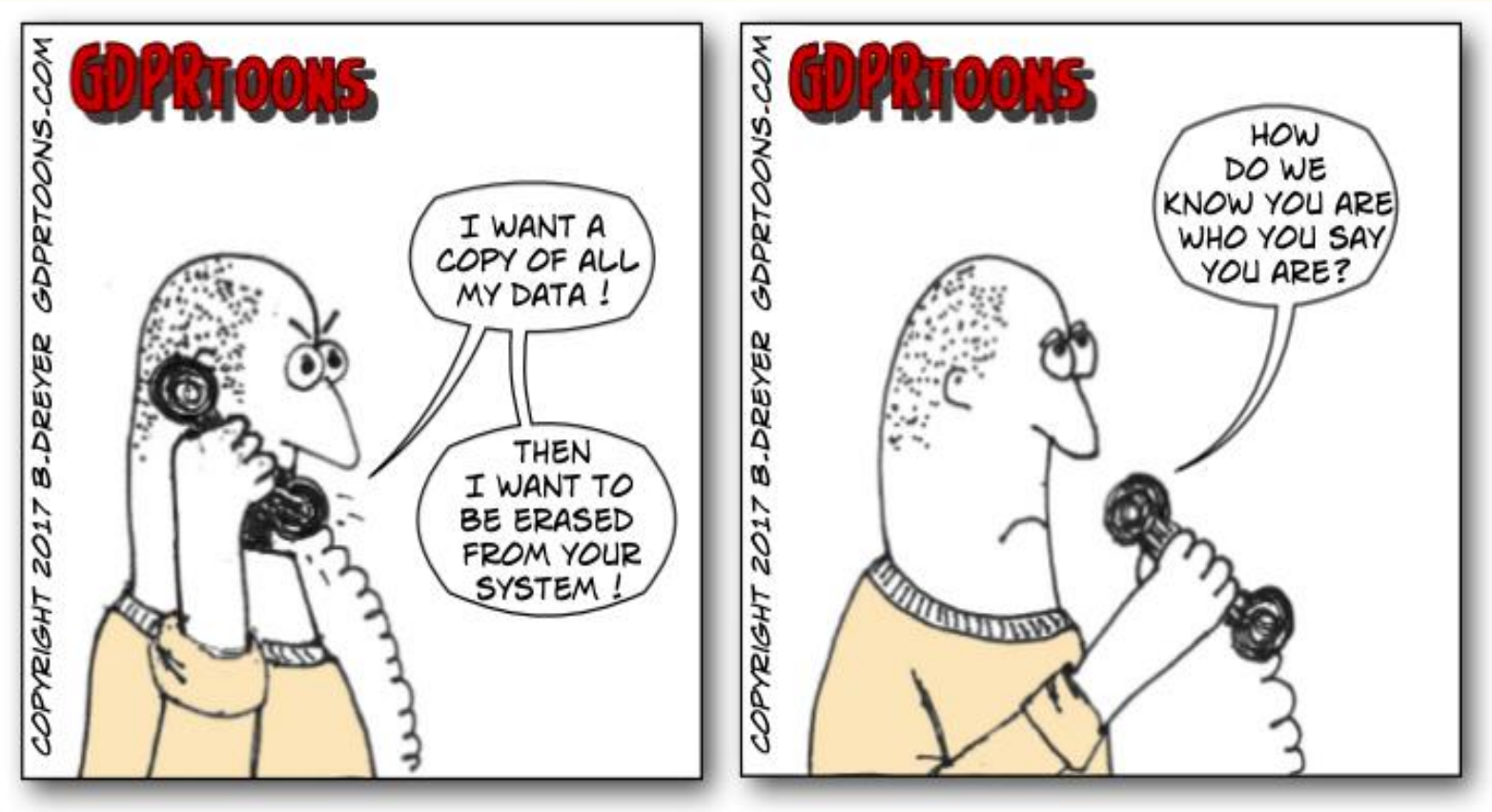
- **On doit veiller à ce que les personnes concernées reçoivent une explication claire du traitement auquel elles consentent ➔ nécessité d'imposer la lecture de la politique de confidentialité et de traitement (Policy) sur les sites Web.**
- **On doit veiller à ce que le mécanisme de consentement soit vraiment volontaire et « opt-in » ➔ case à cocher sur les sites Web et nécessité de détailler les consentements au cas où plusieurs finalités sont envisagées.**
- **On doit permettre aux personnes concernées de retirer leur consentement facilement.**

24 – QUELS SONT LES DROITS DES PERSONNES CONCERNÉES ?

- Droit à l'information
- Droit d'accès
- Droit de rectification
- Droit à la portabilité
- Droit à l'intervention humaine
- Droit à l'oubli
- Droit d'opposition

25 – COMMENT GÉRER LE DROIT A L'INFORMATION ?

- **L'information doit être fournie au moment où les données sont obtenues (si obtenues directement auprès de la personne) ou dans un délai raisonnable (obtenues indirectement).**
- **Il faut préciser en toute transparence quelles données personnelles on traite et la manière dont on les traite (Privacy notice) :**
  - **coordonnées du responsable du traitement et du Data Protection Officer,**
  - **finalités, bases juridiques du traitement et description des intérêts légitimes éventuels – nouvelle information nécessaire en cas de traitement basé sur une autre finalité,**
  - **destinataires éventuels des données et intention éventuelle d'un transfert hors EEE,**
  - **durée de conservation des données ou critères permettant de la déterminer,**
  - **énumération des droits dont disposent les personnes concernées, en ce compris le droit de réclamation,**
  - **conséquence éventuelle de la non fourniture des données.**


GDPRTOONS
COPYRIGHT 2017 B.DREYER GDPRTOONS.COM
I WANT A COPY OF ALL MY DATA !
THEN I WANT TO BE ERASED FROM YOUR SYSTEM !
GDPRTOONS
COPYRIGHT 2017 B.DREYER GDPRTOONS.COM
HOW DO WE KNOW YOU ARE WHO YOU SAY YOU ARE?

26 – COMMENT GÉRER LES DROIT D'ACCÈS ET DE RECTIFICATION ?

- **Droit d'accès**

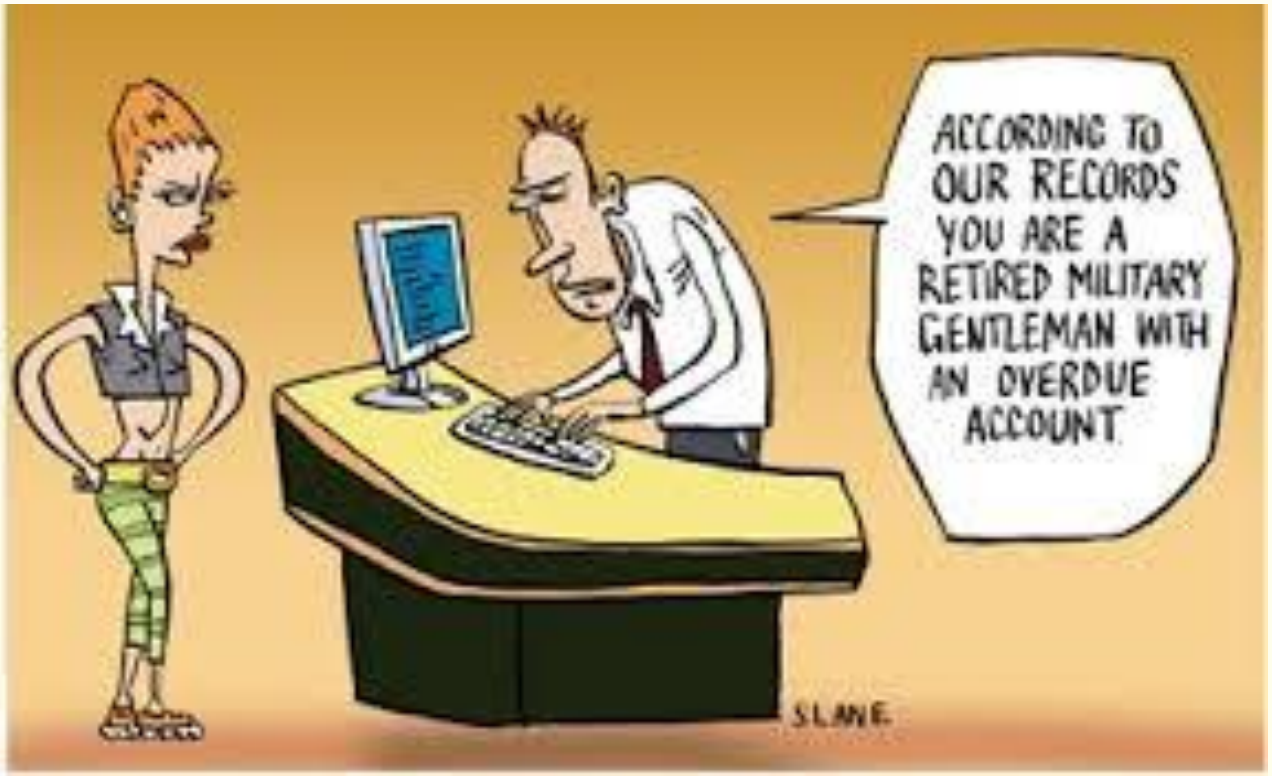
  Lorsque la personne concernée en fait la demande, on doit lui fournir ses données personnelles de manière :

  - **concise, transparente, intelligible et facilement accessible, rédigée en langage clair et facile,**
  - **Gratuitement,**
  - **dans un délai d'un mois (prolongeable de deux mois).**

- **Droit de rectification**

  A la demande de la personne concernée, on doit :

  - **rectifier des données personnelles si elles sont inexactes ou incomplètes,**
  - **informer les tiers si je leur ai communiqué les données personnelles,**
  - **informer les personnes au sujet des tiers auxquels les données ont été divulguées,**
  - **répondre à la personne concernée dans un délai d'un mois (prolongeable de deux mois).**


ACCORDING TO OUR RECORDS YOU ARE A RETIRED MILITARY GENTLEMAN WITH AN OVERDUE ACCOUNT
SLANE

27 – COMMENT GÉRER LE DROIT À LA PORTABILITÉ DES DONNÉES ?

- C’est un des nouveaux droits prévus par le GDPR.
- La personne concernée peut demander de transférer des données personnelles d’un environnement informatique à un autre d’une manière sûre et sécurisée.
- Seules les données personnelles qu’un individu a fournies à un responsable de traitement (sur la base du consentement ou du contrat) sont concernées.
- On doit fournir les données sous une forme structurée, couramment utilisée et lisible.
- On doit le faire gratuitement et dans un délai d’un mois (prolongeable de deux mois).

28 – COMMENT GÉRER LES DROIT D'OUBLI ET D'OPPOSITION ?

- **Droit à l'oubli**
  - La personne concernée peut demander d'être « oubliée » mais ce droit n'est pas absolu.
  - Obligation d'effacement si les données ne sont plus nécessaires, en cas de retrait du consentement qui constituait la base juridique du traitement, si le traitement cause des dommages aux personnes concernées, en cas de traitement illicite.
  - Pour s'opposer à l'effacement des données, il faut justifier d'une obligation légale (prescription), d'une mission d'intérêt public, d'une finalité de recherche scientifique ou historique, de la constatation, l'exercice ou la défense de droits en justice.

➔ **Problématique des Back-up et des DB démultipliées !**

- **Droit d'opposition**
  - La personne concernée peut s'opposer :
    - au direct marketing : lorsque l'on reçoit une demande d'opposition, on doit cesser de traiter immédiatement les données de la personne concernée sans exceptions,
    - au traitement sur la base des intérêts légitimes : lorsque l'on reçoit une opposition, on doit arrêter le traitement de ces données sauf s'il y a des exceptions légales ou à moins de prouver que l'intérêt légitime est à ce point impérieux qu'il contrecarre les droits des personnes concernées,
    - au traitement pour des recherches scientifiques/historiques dans certains cas.
    - On doit informer la personne concernée de son droit de s'opposer dès la première communication et dans la privacy notice.

29 – COMMENT GÉRER LES DONNÉES DES MINEURS ?

- Lorsque la base juridique du traitement repose uniquement sur le consentement de la personne concernée,
- en cas d'offre directe de services de la société de l'information,
- le consentement doit être donné ou autorisé par le titulaire de l'autorité parentale.
- Une fois majeur, l'enfant peut retirer son consentement et s'opposer au traitement.
- Pas de consentement nécessaire en cas de services de prévention ou de conseil.

"Before I write my name on the board, I'll need to know how you're planning to use that data."

30 – COMBIEN DE TEMPS UNE ASSOCIATION PEUT-ELLE CONSERVER DES DONNÉES ?

- **Aucune réponse générale, que des cas particuliers !**
- **Avant toute chose, il faut déterminer le délai de conservation nécessaire pour pouvoir réaliser la finalité du traitement.**
- **Ensuite, il faut répertorier tous les délais légaux de conservation imposés par la loi (prescriptions comptables, fiscales, …) et examiner s'ils sont de nature à prolonger ou le délai de conservation ainsi déterminé.**
- **Enfin, il faut tenir compte des éventuelles procédures judiciaires en cours ou potentielles afin d'en tenir compte pour pouvoir permettre l'exercice des droits en justice.**

31 – QUELLES MESURES DE SÉCURITÉ UNE ASSOCIATION DOIT-ELLE METTRE EN ŒUVRE ?

- **Les mesures de sécurité s'entendent en fonction de l'état des connaissances techniques (article 32 du GDPR).**
- **Elles doivent être proportionnées aux risques encourus et prendre en compte les coûts de mise en œuvre.**
- **Bonnes pratiques**
  - **Minimiser les données traitées : ne récolter que les données strictement nécessaires au but poursuivi.**
  - **Anonymiser autant que faire se peut les données transmises à un tiers et utiliser des connexions sécurisées.**
  - **Sécuriser et limiter les accès aux données.**
  - **Tester régulièrement les mesures mises en œuvre.**
  - **Prévoir des mesures contractuelles avec les sous-traitants et les auditer.**
  - **En cas d'hébergement des données sur un Cloud, vérifier où ce dernier est localisé**

    En cas de localisation hors EEE, nécessité de mesures juridiques adéquates.


TRUST ME. OUR CLOUD SECURITY IS SO GOOD EVEN YOU WON'T BE ABLE TO ACCESS YOUR DATA!
© D.Fletcher for CloudTweaks.com

32 –UNE ASSOCIATION DOIT-ELLE METTRE EN ŒUVRE UNE ANALYSE D'IMPACT (DPIA) ?

L'article 35 du GDPR précise qu'une analyse d'impact est requise

- **en cas de surveillance à grande échelle d'une zone accessible au public,**
- **en cas de traitement à grande échelle de données sensibles ou de données relatives à des condamnations pénales et infractions,**
- **en cas de traitement automatisé des données impliquant une prise de décision automatique produisant des effets juridiques ou affectant de manière significative les personnes concernées,**
- **en cas de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques,**
- **dans les cas déterminés par l'Autorité de protection des données.**

➔ **Hormis ces cas précis, aucune DPIA n'est requise**

33 – COMMENT RÉAGIR EN CAS DE DATA BREACH ?

- **Notion de Data breach : destruction, perte, altération, divulgation non autorisée, accès non autorisé accidentels ou illicites.**
- **Organiser la remontée de tous les incidents de type Privacy.**
- **Analyser les défaillances constatées.**
- **Définir des mesures de remédiation.**
- **Organiser la procédure d'information de l'autorité de contrôle : délai de 72h à compter du constat sauf si aucun risque pour les droits et libertés des personnes concernées.**
- **Définir et mettre en œuvre un plan de communication vers la clientèle en cas de Data breach majeure.**

34 – COMMENT MENER UN PROJET GDPR ?

DEMARCHE DE LA CPVP EN 13 ETAPES

1. Conscientiser (Décideurs et collaborateurs)
2. Etablir un registre des données (Inventaire des données traitées et partagées)
3. Communiquer (avec les personnes concernées)
4. Gérer les droits des personnes concernées
5. Mettre à jour les procédures d'accès existantes
6. Définir le fondement légal des traitements
7. Evaluer comment demander, obtenir et conserver le consentement des personnes concernées
8. Prévoir un régime spécifique pour les enfants
9. Déterminer les procédures pour détecter, rapporter et analyser les fuites de données
10. Protéger les données dès la conception et l'analyse d'impact
11. Nommer un délégué à la protection des données
12. Examiner si votre organisme est actif au niveau international
13. Revoir tous les contrats existants avec les sous-traitants

34 – COMMENT MENER UN PROJET GDPR ?

DEMARCHE DE LA CNIL EN 6 ETAPES

1. Désigner un pilote

- Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

2. Cartographier vos traitements de données personnelles

- Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

3. Prioriser les actions à mener

- Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

4. Gérer les risques

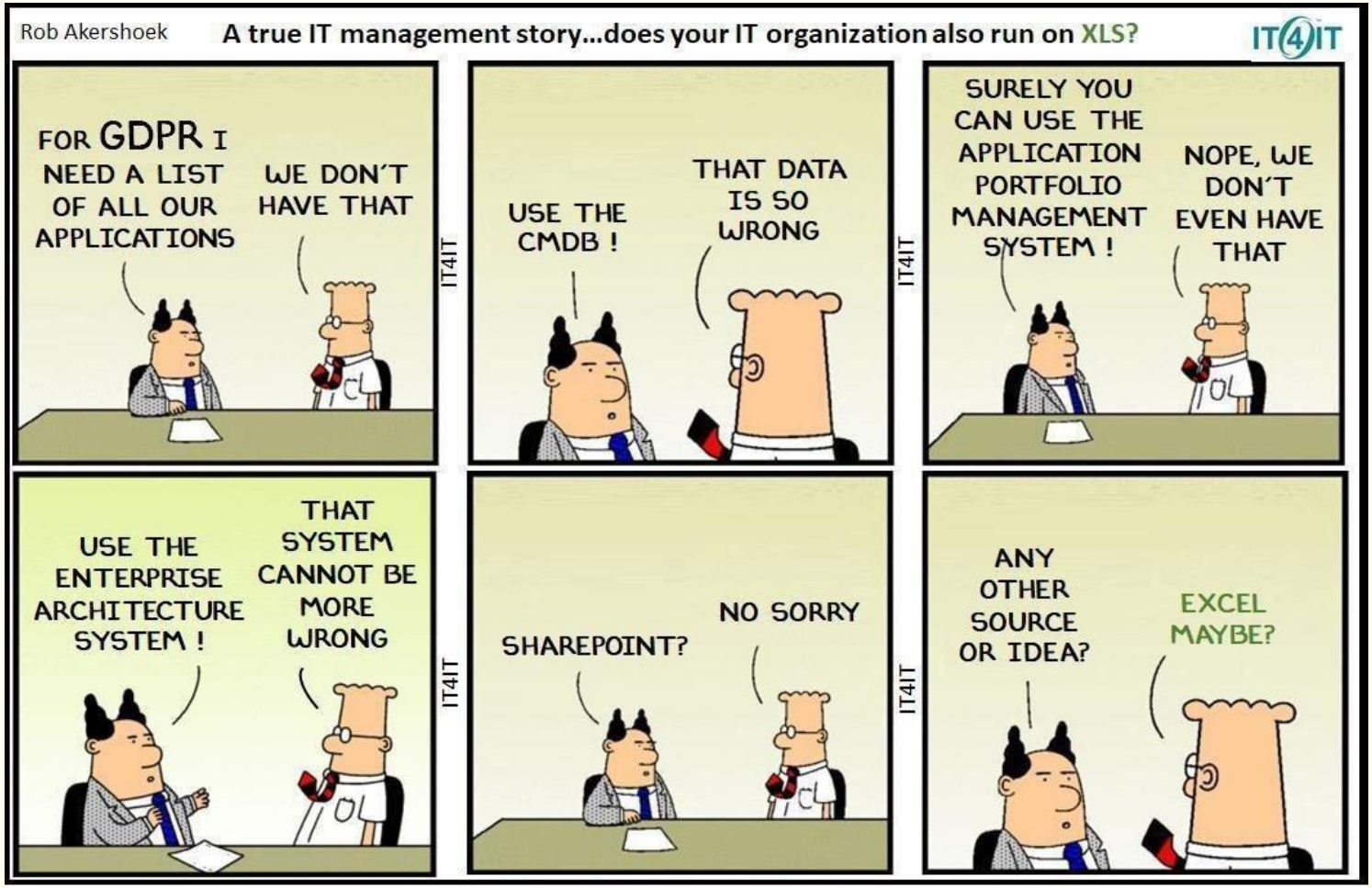
- Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données

5. Organiser les processus internes

- Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

6. Documenter la conformité

- Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.


Rob Akershoek
A true IT management story...does your IT organization also run on XLS?
IT4IT
FOR GDPR I NEED A LIST OF ALL OUR APPLICATIONS
WE DON'T HAVE THAT
IT4IT
USE THE CMDB !
THAT DATA IS SO WRONG
IT4IT
SURELY YOU CAN USE THE APPLICATION PORTFOLIO MANAGEMENT SYSTEM !
NOPE, WE DON'T EVEN HAVE THAT
USE THE ENTERPRISE ARCHITECTURE SYSTEM !
THAT SYSTEM CANNOT BE MORE WRONG
IT4IT
SHAREPOINT?
NO SORRY
IT4IT
ANY OTHER SOURCE OR IDEA?
EXCEL MAYBE?

35 – QUELLES SANCTIONS EN CAS DE NON RESPECT DU GDPR ?

- **Sanctions**
- 17 mesures possibles: classement sans suite, non-lieu, conciliation, avertissement, interdiction temporaire, astreinte, communication au parquet, publication de la décision, amende administrative, etc.
- Amende administrative: pouvant aller jusqu'à 10 ou 20,000,000 € !
- Recours possible: cour des marchés

- **Autorité de protection des données (ancienne CPVP)**
  - Médiateur de la protection des données: examen des plaintes
  - Service d'inspection: organe d'enquête; larges pouvoirs d'investigation (officiers de police judiciaire)
  - Mesures provisoires possibles (**suspension du traitement**…)
  - Chambre contentieuse

SITES INTERNET UTILES

- **CNIL**
  - https://www.cnil.fr/professionnel
- **BCSS**
  - **https://www.ksz-bcss.fgov.be/fr/securite-et-vie-privee/general-data-protection-regulation**
- **CPVP**
  - **https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees-0**
- **Article 29 Working party**
  - **http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083**
- **Portail européen**
  - **http://www.eugdpr.org/eugdpr.org.html**

Logiciel « Elea Software »

Présentation « Elea conseil »

Nos domaines d'expertise :

- Normes ISO (10 ans)
- ISO 27001 Management de la sécurité de l'information (4 ans)
- GDPR (1an)

Présentation « Elea conseil »

Partenaire avec l'Université de Liège – ULG

Développement de modules futurs :

- Analyses des risques / impacts
- ISO 27001
- …

Présentation « Elea conseil »

Notre équipe d'experts GDPR :

- Experts « Juridique »
- Experts « IT » Sécurité de l'information
- Experts « Management d'entreprise »

Synergie des 3 compétences « clés » pour une mise en conformité au GDPR efficace

Présentation « Elea conseil »

Notre expérience a identifié un réel besoin de créer un logiciel :

- Comprendre la logique du GDPR
- Structurer la mise en conformité au GDPR / Maintien de la conformité
- Outil de gestion des données personnelles (reporting)
- Permet une réponse structurée aux différentes demandes des personnes concernées (Droit à l'oubli, …)

Séance QUESTIONS - RÉPONSES

- Sophie DENOOZ, Conseillère juridique AISF
- Dominique COUNASSE, Coordination transversale Ethias
- Florence LACROSSE, Directrice Elea Software

Séance animée par Serge MATHONET, Directeur AISF

Merci

Place au lunch et au verre de l'amitié dans l'espace cafeteria

Mardi 21 octobre 2014
Parlement de la Fédération Wallonie-Bruxelles

AISF Association Interfédérale du Sport Francophone