Le Règlement Général sur la Protection des Données (« RGPD »)

- Bertrand FRANCK
- Avocat au Barreau de Liège
- Certificat en Protection des Données (Data Protection Institute)
- bfranck@bdaa.be

- Avenue Louis Libert 31, 4920 Aywaille
- 04/384.84.64
- info@bdaa.be
- www.bdaa.be
- www.rgdp.be

I. INTRODUCTION

De quoi parle-t-on ?

Règlement **G**énéral sur la **P**rotection des **D**onnées

I. INTRODUCTION

Règlement Européen 2016/679 (+ Directive 2016/680 & Loi belge à intervenir)

Adopté le 14 avril 2016

Applicable depuis le 25 mai 2018

I. INTRODUCTION

Protection des données ?

-> Vise la protection des données dites « ***à caractère personnel*** »

=/ Protection de la vie privée

I. INTRODUCTION

- Pourquoi protéger les données à caractère personnel?
- Les données à caractère personnel ont de la valeur pour de nombreux acteurs
- Les technologies évoluent rapidement
- Les risques dépendent du contexte et du type de données

I. INTRODUCTION

31 Mars 2017 :

Alphabet (Google) était la deuxième plus grande entreprise mondiale d'un point de vue capitalisation boursière (579 milliards $ en mars 2017, 766,67 milliards en février 2018)

Facebook était 6ème.

/ Données personnelles / Risques

Que font les cybercriminels des données dérobées ?

Base de données	Usurpation d'identité
• Spam • Appels indésirés • Courriers publicitaires • …	• Se faire passer pour X afin d'arnaquer Y • Souscrire à des services en se faisant passer pour X • Appeler la victime en se faisant passer pour un tiers de confiance grâce aux données personnelles détenues

/ Données personnelles / Fuites

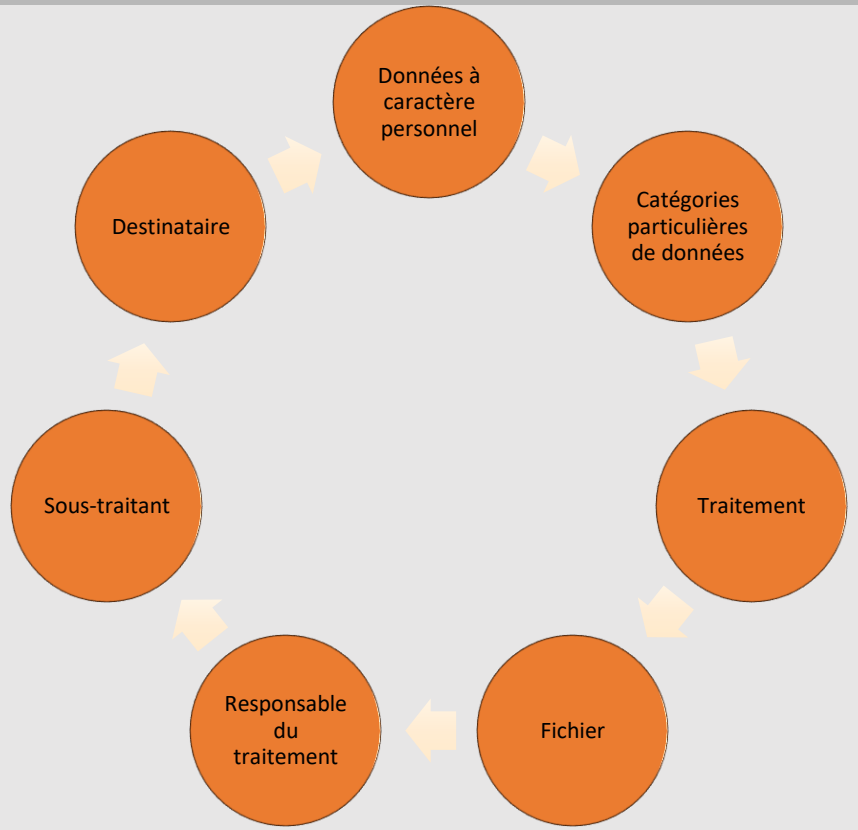
2014 – Orange (France / Opérateur télécom) se fait dérober les données personnelles de 1,3 millions de clients

- (prénom, nom, date de naissance, email, numéro de téléphone)

2012 – Un annuaire de la Défense a fuité

- Document de 37 pages reprenant le grade, nom, numéro professionnel et adresse email de 500 collaborateurs de la Défense

II. DEFINITIONS



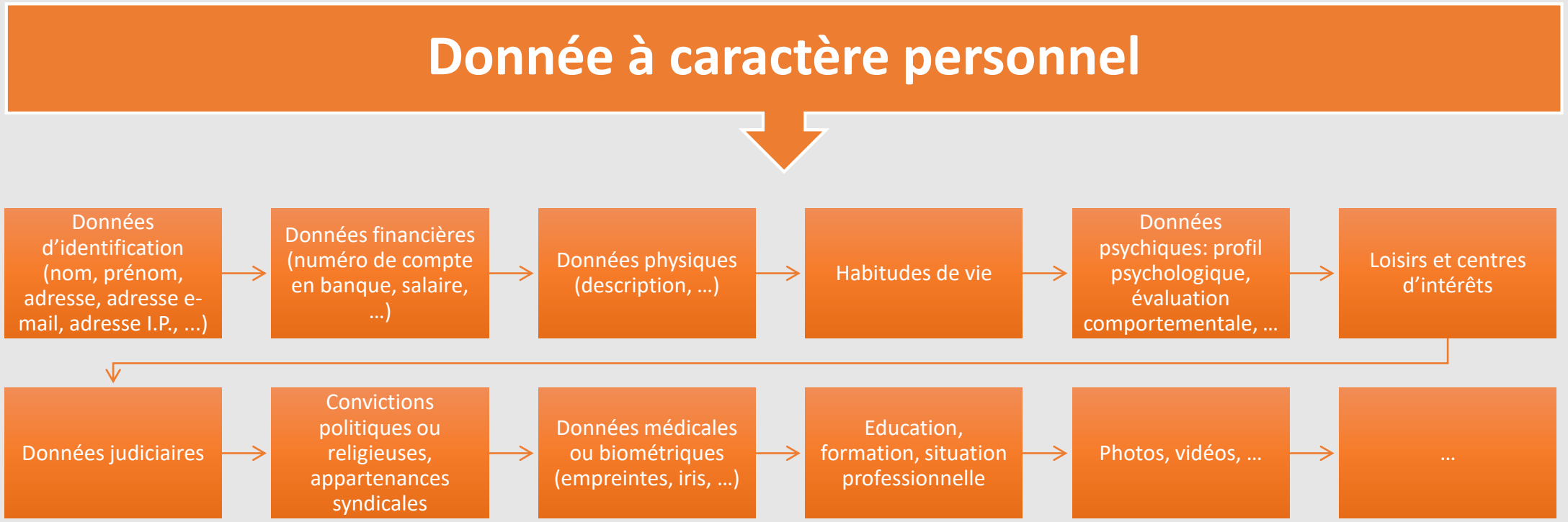
II. DEFINITIONS

Donnée à caractère personnel

= « *toute information se rapportant à une personne physique identifiée ou identifiable* »

Toute information = donnée, information, connaissance, peu importe la forme ou le contenu	Se rapportant à = plus large que *portant sur*	Personne physique = vivante, et pas une personne morale (sauf si celle-ci renvoie directement à une personne physique)	Identifiée, ou identifiable directement ou indirectement (en considération des moyens raisonnablement susceptibles d'être utilisés)

II. DEFINITIONS



II. DEFINITIONS

Catégories particulières de données:

> Données à caractère personnel « *sensible* », qui *révèlent*:

- L'origine raciale ou ethnique;
- Les opinions politiques;
- Les convictions religieuses, philosophiques, ou l'appartenance syndicale

> Ou qui portent sur / concernent:

- La vie sexuelle
- L'orientation sexuelle d'une personne physique

REVELER =/ PORTER SUR / CONCERNER

II. DEFINITIONS

Traitement:

« toute opération 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»

- Automatisé = informatiquement
- Si pas automatisé : notion de « fichier »

= 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 de données

II. DEFINITIONS

Traitement:

« Finalités du traitement »

Candidature/ Recrutement	Gestion des carrières	Paie	Vie du salarié	Logistique	Sécurité/logistique
• Entretiens • Tests/évaluation	• Formation • Evaluation annuelle • Mobilité • Sanctions disciplinaires	• Gestion des fiches de paie • Comptabilité	• Relations sociales (élection du personnel, syndicat)	• Gestion de la téléphonie / matériel informatique • Véhicule professionnel	• Badge • vidéosurveillance

II. DEFINITIONS

Fichier:

« tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »

- Dossiers « papier » classés
- Fardes
- Dossiers suspendus
- …

II. DEFINITIONS

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* »

- Notion de fait, en principe l'entreprise, l'association, l'autorité publique ou l'organisme.

- Il peut y avoir plusieurs responsables du traitement

- Généralement pas une personne physique, mais un organe (conseil d'administration, ministre, …)

II. DEFINITIONS

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 »

- Il agit sur les instructions du R.T.
- Régime particulier de responsabilités et d'obligations
- Par exemple: hébergeur, fournisseur de services « cloud » ou e-mail, secrétariat social, comptable, partenaire…

II. DEFINITIONS

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»

- = Tiers, sous-traitant, administration, …
- Tiers = toute personne autre que la personne concernée, le R.T., le S.T. et leurs préposés

III. CHAMP D'APPLICATION

Matériel : Quoi ?

Deux critères:

- *Traitement (automatisé ou non)*
- *De données à caractère personnel*

Territorial: où ?

Le RGPD s'applique:

- à l'établissement situé sur le territoire de l'Union Européenne (R.T. ou S.T.);
- si les personnes concernées situées sur le territoire de l'Union Européenne

Champ d'application extrêmement large

- Notions de traitement et de DCP très larges

- Champ d'application territorial étendu

III. CHAMP D'APPLICATION

Exceptions

- Le RGPD **ne** s'applique **pas**:
- Aux traitements effectués dans le cadre d'une activité qui ne relève pas du champ d'application du droit U.E.
- Aux traitements effectués par les états membres dans le cadre d'activités qui concernent la P.A.C.
- Aux traitements effectués dans le cadre d'une activité strictement personnelle ou domestique
- Aux traitements effectués par la police et la justice pour prévenir, détecter, poursuivre et punir les infractions pénales (-> directive *ad hoc* « Police & Justice »)
- Aux traitements réalisés par les autorités européennes (-> règlement 45/2001, doit être conforme au RGPD)

III. CHAMP D'APPLICATION

Dérogations:

- Le RGPD **ne** s'applique **pas <u>entièrement:</u>**
  -Lorsque des lois le prévoient et qu'il s'agit de protéger des matières touchant à la sécurité nationale, la défense, …
  -Dans le cadre de traitements réalisés à des fins journalistiques, scientifiques, historiques, statistiques, archivistiques...
- Certains articles ne s'appliquent pas pour coller aux spécificités de ces activités (droit à l'effacement / l'oubli / …)

IV. PRINCIPES RELATIFS AU TRAITEMENT

- Principe de licéité (+ loyauté et transparence)
- Principe de limitation des finalités
- Principe minimisation des données
- Principe d'exactitude des données
- Principe de limitation de la conservation
- Principe d'intégrité et de confidentialité
- Principe de responsabilité (*accountability – démontrabilité)*

IV. PRINCIPES RELATIFS AU TRAITEMENT

1) LICEITE / Bases de légitimation

Elles sont au nombre de six:

- Le consentement
- La relation contractuelle
- L'obligation légale
- L'intérêt vital
- L'intérêt public (autorité publique)
- L'intérêt légitime du responsable du traitement ou du tiers

IV. PRINCIPES RELATIFS AU TRAITEMENT

BASE DE LÉGITIMATION : LA RELATION CONTRACTUELLE

- Conditions:
  - La personne concernée est partie au contrat ;
  - Le traitement est nécessaire à l'exécution du contrat (Ex: faire de la publicité n'est jamais nécessaire à l'exécution du contrat)
- Cela peut aussi concerner des mesures préalables au contrat (étude de solvabilité préalable à crédit, …)

IV. PRINCIPES RELATIFS AU TRAITEMENT

BASE DE LÉGITIMATION : L'OBLIGATION LEGALE

- *« Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »*
- L'obligation légale en question doit relever du droit national d'un pays.
- Exemple: obligations de transmettre des données pour lutter contre le blanchiment, au fisc, aux assureurs, ...

IV. PRINCIPES RELATIFS AU TRAITEMENT

BASE DE LÉGITIMATION : INTÉRÊT VITAL

- *« Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne*
- *physique »*

- **Conditions:**
  - L'intérêt est vital, il y a une vie en danger
  - Aucun autre fondement n'est pas possible

- **Cas typique:** transfert de données entre hôpitaux, en cas d'urgence

IV. PRINCIPES RELATIFS AU TRAITEMENT

BASE DE LÉGITIMATION : INTÉRÊT PUBLIC

- Le traitement est nécessaire à :
  - L'exécution d'une mission d'intérêt public;
  - L'exécution d'une mission relevant de l'exercice de l'autorité publique dont est investi le
- responsable du traitement

- Notion de fait : Mission d'intérêt public ou non?

IV. PRINCIPES RELATIFS AU TRAITEMENT

BASE DE LÉGITIMATION : INTÉRÊTS LÉGITIMES DU R.T.

- Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, **à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la P.C.**.
- Mise en balance des intérêts du responsable par rapport à ceux de la personne concernée
- Exemple: liberté d'entreprise, droit à l'information, …

IV. PRINCIPES RELATIFS AU TRAITEMENT

BASE DE LÉGITIMATION : LE CONSENTEMENT

- La personne concernée a **consenti** au traitement de ses données à caractère personnel pour une ou plusieurs finalités **spécifiques et clairement énoncées (transparence et information).**
- **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 »*

IV. PRINCIPES RELATIFS AU TRAITEMENT

LICEITE: CATEGORIES PARTICULIERES DE DONNEES

- **Traitement en principe interdit, sauf dans dix cas** (et il faut toujours une base de légitimation)
- 1) Si la P.C. a donné son consentement
- 2) Exécution d'obligations et de droits en matière de droit du travail ou de sécurité sociale
- 3) Pour la sauvegarde d'intérêts vitaux de la P.C. ou d'une autre personne, si pas possible d'avoir le consentement
- 4) Gestion des membres (Fondation, association, etc. poursuivant une finalité politique, philosophique, religieuse)
- 5) Données rendues publiques
- 6) Constatation, exercice ou défense d'un droit en justice
- 7) Motifs d'intérêt public important
- 8) Contexte de soins de santé
- 9) Motifs d'intérêt public dans le domaine de la santé publique (menaces transfrontalières)
- 10) Archivage dans l'intérêt public, recherche scientifique ou historique, statistiques

IV. PRINCIPES RELATIFS AU TRAITEMENT

2) LIMITATION DES FINALITÉS

2.1) Principe de finalité: *« les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes »* : pas de finalités secrètes, elles doivent être décrites explicitement et légitimes (par rapport à l'objet social du responsable du traitement, par exemple)

2.2) Principe de compatibilité: *« les données à caractère personnel ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités »*

IV. PRINCIPES RELATIFS AU TRAITEMENT

3) MINIMISATION DES DONNÉES

Les DCP traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées

On ne traite pas une donnée si ce n'est pas nécessaire

Exemples:

Numéro de compte bancaire dans un processus de recrutement;

Extrait de casier judiciaire pour un recrutement à une fonction simple (sans exigence de moralité spécifique)

Numéro de registre national d'un client

IV. PRINCIPES RELATIFS AU TRAITEMENT

4) EXACTITUDE DES DONNEES

Toutes les mesures **raisonnables** doivent être prises pour que les DCP qui sont inexactes, eu égard aux finalités pour

lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder

(Obligation de moyens)

IV. PRINCIPES RELATIFS AU TRAITEMENT

5) LIMITATION DE LA DUREE DE CONSERVATION

Les DCP doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour

Lesquelles elles sont traitées

On ne peut pas conserver pour conserver

(Possibilité d'anonymiser – intérêt limité)

IV. PRINCIPES RELATIFS AU TRAITEMENT

6) INTÉGRITÉ ET CONFIDENTIALITÉ

Intégrité = sécurité, disponibilité + Confidentialité

Les DCP doivent être traités de façon à garantir « une *sécurité appropriée de DCP, y compris contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle,* à *l'aide de* ***mesures techniques et organisationnelles appropriées »***

IV. PRINCIPES RELATIFS AU TRAITEMENT

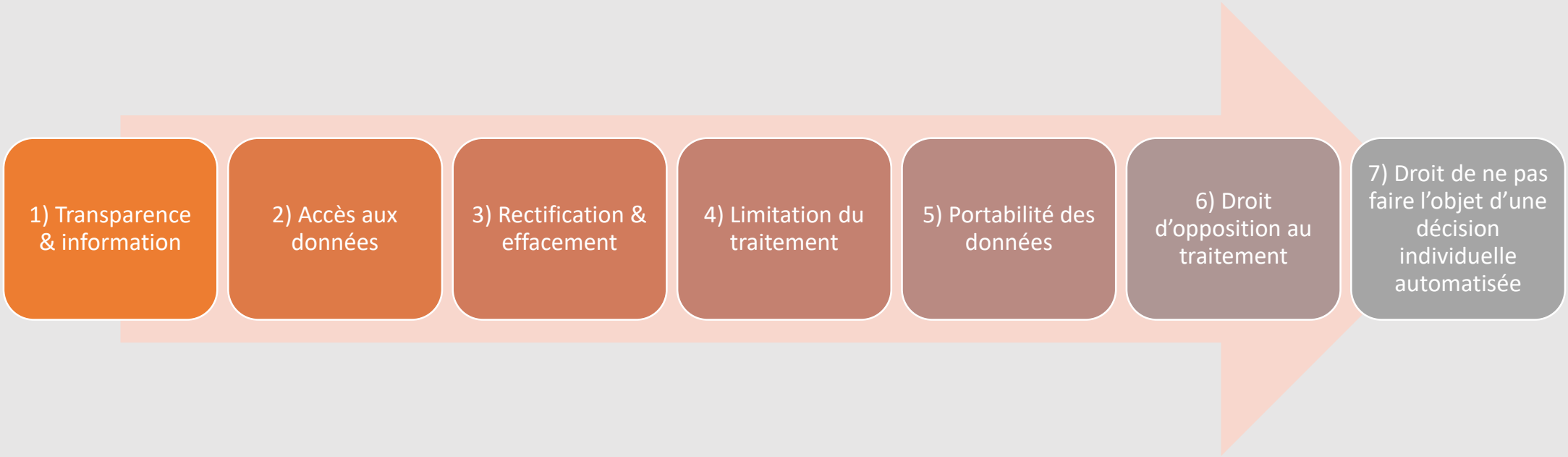
7) RESPONSABILITÉ - *ACCOUNTABILITY*

Le responsable du traitement est responsable du respect des six autres principes, et doit être en tout temps capable de démontrer qu'il les respecte bien

La charge de la preuve repose sur le responsable du traitement

Importance de documenter sa mise en conformité

V. DROITS DE LA PERSONNE CONCERNÉE



V. DROITS DE LA PERSONNE CONCERNEE

DROIT : TRANSPARENCE ET INFORMATION

- Le responsable du traitement doit faire preuve de transparence à l'égard des DCP qu'il traite, des finalités des traitements réalisés, de la durée de conservation de ces données, … (Liste des informations à fournir: article 13)
- Le R.T. doit informer les personnes concernées de manière *« concise, transparente, compréhensible, et aisément accessible »*.
- Le R.T. doit assurer le respect de ces droits, et prendre *« les mesures appropriées »* en ce sens.
- Le R.T. donne suite aux demandes des personnes concernées dans le mois.

V. DROITS DE LA PERSONNE CONCERNEE

DROIT : ACCES AUX DONNEES

- *« La PC a le droit d'obtenir du responsable du traitement la confirmation que des DCP la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites DCP ainsi que les informations suivantes:*
- *a) les finalités du traitement;*
- *b) les catégories de données à caractère personnel concernées;*
- *c) les destinataires ou catégories de destinataires auxquels les DCP ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales;*
- *d) lorsque cela est possible, la durée de conservation des DCP envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;*
- *e) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de DCP, ou une limitation du traitement des DCP relatives à la personne concernée, ou du droit de s'opposer à ce traitement;*
- *f) le droit d'introduire une réclamation auprès d'une autorité de contrôle;*
- *g) lorsque les DCP ne sont pas collectées auprès de la PC, toute information disponible quant à leur source;*
- *h) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, les informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.*

V. DROITS DE LA PERSONNE CONCERNEE

DROIT : RECTIFICATION ET EFFACEMENT

- *« La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. »*

V. DROITS DE LA PERSONNE CONCERNEE

DROIT : RECTIFICATION ET EFFACEMENT

- La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des DCP la concernant et le responsable du traitement a l'obligation d'effacer ces DCP dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:
- a) les DCP ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;
- b) la PC retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement;
- c) la PC s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2;
- d) les DCP ont fait l'objet d'un traitement illicite;
- e) les DCP doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;
- f) les DCP ont été collectées dans le cadre de l'offre de services de la société de l'information

V. DROITS DE LA PERSONNE CONCERNEE

DROIT : LIMITATION DU TRAITEMENT

- Suspension temporaire du traitement de certaines DCP lorsque:

- a) l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel;
- b) le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation;
- c) le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice;
- d) la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

V. DROITS DE LA PERSONNE CONCERNEE

DROIT : PORTABILITE DES DONNEES

- Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque:
- a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9,paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b); **et**
- b) le traitement est effectué à l'aide de procédés automatisés.

V. DROITS DE LA PERSONNE CONCERNEE

DROIT : OPPOSITION AU TRAITEMENT

- *« La personne concernée **a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière**, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, **point e) ou f),** y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. »*

- *« Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection. »*

V. DROITS DE LA PERSONNE CONCERNEE

DROIT : DROIT DE NE PAS FAIRE L'OBJET D'UNE DECISION INDIVIDUELLE AUTOMATISEE

- *« La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. »*

- SAUF:

  - Consentement,
  - Nécessité pour l'exécution du contrat,
  - Expressément autorisé par une loi qui prévoit des garde-fous suffisants

VI. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

1. Mise en œuvre de mesures techniques et organisationnelles appropriées, et d'une politique adéquate (responsabilité & sécurité)
2. Vigilance dans le choix des sous-traitants
3. Notification des violations
4. Tenue d'un registre des activités de traitement
5. Réalisation d'une analyse d'impact
6. Désignation d'un délégué à la protection des données
7. « Privacy by Design » / « Privacy by Default »
8. Obligations en matière de transferts de données

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

MESURES TECHNIQUES ET ORGANISATIONNELLES

- Deux aspects:

  - En vue de satisfaire au principe de **RESPONSABILITÉ**;
  - En vue d'assurer la **SÉCURITÉ et la CONFIDENTIALITÉ** des données et des traitements

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

VIGILANCE DANS LE CHOIX DES SOUS-TRAITANTS

- Si le R.T. doit confier à des sous-traitants le traitement de DCP, le R.T. a l'obligation de s'assurer que le S.T. offre des garanties suffisantes aux personnes concernées
- Vérifier que le S.T. est bien *compliant*
- Le R.T. sera tenu pour responsable d'une violation survenue en raison de la non-conformité du S.T. au RGPD!
- Obligation d'établir un contrat comprenant certaines clauses (modèle CNIL)

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

NOTIFICATION DE VIOLATION DES DONNÉES

- Notification de toute violation dans les 72H de la prise de connaissance, sauf si cette violation n'est pas susceptible d'engendrer un risque pour les droits et libertés
- Notification à l'autorité de contrôle et aux personnes concernées.
- Exemple: piratage informatique, vol de données, perte d'un ordinateur portable, d'une clé usb…

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

TENUE D'UN REGISTRE DES ACTIVITÉS DE TRAITEMENT

- *« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:*
- *a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;*
- *b) les finalités du traitement;*
- *c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;*
- *d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;*
- *e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;*
- *f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;*
- *g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelle visées à l'article 32, paragraphe 1. »*

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

TENUE D'UN REGISTRE DES ACTIVITÉS DE TRAITEMENT

- *« Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf :*
  - *si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées,*
  - *s'il n'est pas occasionnel*
  - *s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »*

- **IL FAUT (PRATIQUEMENT) <u>TOUJOURS</u> UN REGISTRE DU TRAITEMENT**

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

REALISATION D'UNE ANALYSE D'IMPACT

- *« Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. »*

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

REALISATION D'UNE ANALYSE D'IMPACT

- *« L'analyse contient au moins:*
- *a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;*
- *b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;*
- *c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et*
- *d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. »*

- Une liste sera établie par l'autorité de contrôle

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

DESIGNATION D'UN DELEGUE A LA PROTECTION DES DONNÉES

- Le DPD est:

  - La personne de contact et de référence pour l'autorité de contrôle et les personnes concernées;
  - Le pilote de la mise en conformité de son organisation;
  - Chargé d'informer et de conseiller le R.T. ;
  - Chargé de documenter en vue de satisfaire au principe de responsabilité;
  - Chargé de contrôler la conformité des activités du R.T. au RGPD.

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

DESIGNATION D'UN DELEGUE A LA PROTECTION DES DONNÉES

- *« Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:*
- *a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;*
- *b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou*
- *c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »*

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

DESIGNATION D'UN DELEGUE A LA PROTECTION DES DONNÉES

- Le DPD peut être **soit interne, soit externe** (avocat, consultant, …) à l'organisation du responsable du traitement.
- Il **doit** disposer de *« connaissances spécialisées du droit et des pratiques en matière de protection des données ».*
- Il **ne** peut **pas faire partie du management** (poste décisionnel), car il y aurait risque de conflit d'intérêt.
- Il **ne** peut **pas** être désigné parmi des employés sous **contrat à durée déterminée (courte).**
- Il fait l'objet d'une **protection contre le licenciement** dans le cadre de ses activités de DPD.
- Le R.T. doit mettre à sa disposition **le temps et les ressources nécessaires** à l'exercice de sa mission.
- Il doit idéalement avoir une position **sous le management direct** dans l'organigramme.

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

PRIVACY BY DESIGN / PRIVACY BY DEFAULT

- « *Privacy* » dès la conception: tenir compte du RGPD dès la conception de nouveaux processus, logiciels, plateformes, … afin que ceux-ci assurent *dans la manière dont ils sont conçus*, la possibilité de respecter le RGPD et d'assurer le respect des droits des P.C.

- « *Privacy* » par défaut: *par défaut*, il faut proposer les options les plus protectrices des droits des PC (incidences en matière de cookies, de profils, de newsletter, …)

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

TRANSFERT DE DONNEES

- *« **Un transfert**, vers un pays tiers ou à une organisation **internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si,** sous réserve des autres dispositions du présent règlement, **les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale**. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis. »*

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

TRANSFERT DE DONNEES

- Transfert fondé sur une décision d'adéquation (UE + « White List »: Argentine, Andorre, Canada, Etats-Unis *(Privacy Shield),* Guernesey, Ile de Man, Iles FEROE, Israël, Jersey, Nouvelle-Zélande, Suisse, Uruguay)

- Transfert offrant des garanties suffisantes (clauses-types ou règles d'entreprise contraignantes – *binding corporate rules*

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

SANCTIONS

- *Sanctions par l'Autorité de Protection des Données:*

  - Administratives (injonctions)

  - Financières (amendes): jusqu'à 4% du chiffre d'affaire annuel mondial, ou jusqu'à 20 millions d'euro (plafond le plus élevé)

- *Sanctions connexes*

  - Perte de contrats et de marchés publics;
  - Perte de subsides (exigences des organismes subsidiant)
  - Risque de contentieux important

VI. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

SANCTIONS

- L'autorité de contrôle:
- En Belgique, AUTORITÉ DE PROTECTION DES DONNÉES (ancienne Commission de Protection de la Vie Privée).

- Plusieurs missions:

  - Réception des plaintes et informations des citoyens;

  - Assistance des responsables de traitements et des sous-traitants;

  - Dispense de conseils et de recommandations;

  - Inspection, contrôle et sanctions.

VII. MISE EN CONFORMITÉ – ASPECT PRATIQUE

ETAPES DE LA MISE EN CONFORMITÉ

- **DESIGNER UN PILOTE DE LA MISE EN CONFORMITÉ – ETABLIR UNE STRATEGIE ET UNE POLITIQUE DE PROTECTION DES DCP**
- **SENSIBILISER, INFORMER ET FORMER À LA PROTECTION DES DONNÉES**
- **CARTOGRAPHIER LES DCP ET LES TRAITEMENTS – ETABLIR LE REGISTRE**
- **AUDIT DES RISQUES (+ DPIA?)**
- **HIERARCHISER LES ACTIONS À ENTREPRENDRE**
- **ORGANISER LES PROCESSUS INTERNES: politique de gestion des incidents, politique de traitement en matière de droit d'accès, de data breach, …**
- **DOCUMENTER LA MISE EN CONFORMITÉ**

VII. MISE EN CONFORMITÉ – ASPECT PRATIQUE

ETAPES DE LA MISE EN CONFORMITÉ

- Etablir un registre du traitement
- Désignation d'un délégué à la protection des données
- Identifier les sous-traitants et revoir les contrats
- Adapter les contrats de travail & le règlement de travail (confidentialité)
- Prendre les mesures organisationnelles évidentes et simples pour remédier aux risques principaux

VII. MISE EN CONFORMITÉ – ASPECT PRATIQUE

MISE EN CONFORMITÉ – ASPECTS PRATIQUES

Modèles :

- Registre des activités de traitement;
- Contrat de sous-traitance;
- Politique de confidentialité interne;
- Politique de confidentialité;
- Déclarations cookies;
- …

VII. MISE EN CONFORMITÉ – ASPECT PRATIQUE

RESSOURCES

- Commission de la protection de la vie privée (CPVP)
  Modèle de registre des activités de traitement
  Une partie de leur site est dédiée à RGPD
- CNIL (équivalent français du CPVP)
  Logiciel libre pour réaliser des analyses d'impact
- Centre de la Cybersécurité Belgique (CCB)
  Guide sur la cybersécurité
  GDPR CheckUp : vidéos, informations, quizz… (20 minutes)

Questions - Réponses

Merci pour votre attention!

Cabinet d'avocats Balthasar & Delrée - info@bdaa.be - www.bdaa.be - www.rgdp.be