Les grandes lignes du Règlement général sur la protection des données

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Franck Dumortier

Franck.dumortier@unamur.be

Structure

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

1. Cadre légal applicable
2. Champ d'application
3. Principes relatifs au traitement de données à caractère personnel
4. Licéité du traitement
5. Conditions applicables au consentement
6. Catégories particulières de données
7. Droits de la personne concernée
8. Obligations du responsable du traitement et du sous-traitant
9. Divers

1. Cadre légal applicable

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Actuellement

- **Convention n°108** du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (1981) (Voir ici)
- **Directive 95/46/CE** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Voir ici)
- **Loi du 8 décembre 1992** relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. (Voir ici)

25 mai 2018

- **Règlement général sur la protection des données** (« GDPR ») du 27 avril 2016 (abrogeant la directive 95/46/CE). (Voir ici)

2. Champ d'application

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Champ d'application matériel :

- tout **traitement** : une opération ou un ensemble d'opérations effectuées à l'aide ou non de procédés automatisés
- de **données à caractère personnel** : information qui concerne une personne physique identifiée ou identifiable
- automatisé : **tout en partie ou non automatisé** mais contenues/appelées à figurer dans un **fichier**

>< traitement à des fins personnelles ou domestiques

>< police, justice, etc.

+ règles spécifiques prévues par le droit national (CCT, numéro d'identification national, etc.)

2. Champ d'application

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Champ d'application territorial :

- RT/ST **est établi sur le territoire de l'UE**, indépendamment du lieu du traitement (dont secteur public)

- RT/ST n'est pas établi dans l'UE et que les **personnes concernées se trouvent sur le territoire de l'UE** (pas applicable au secteur public !)

  → obligation de désigner par écrit un Rep au sein de l'Union

Remarques

RT : **« responsable du traitement »:** la PP ou PM qui seule ou conjointement avec d'autres, détermine les **finalités** et les **moyens** du traitement

ST : **« sous-traitant »:** la PP ou PM qui traite des données à caractère personnel pour le compte du responsable du traitement

3. Principes relatifs au traitement des données à caractère personnel

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

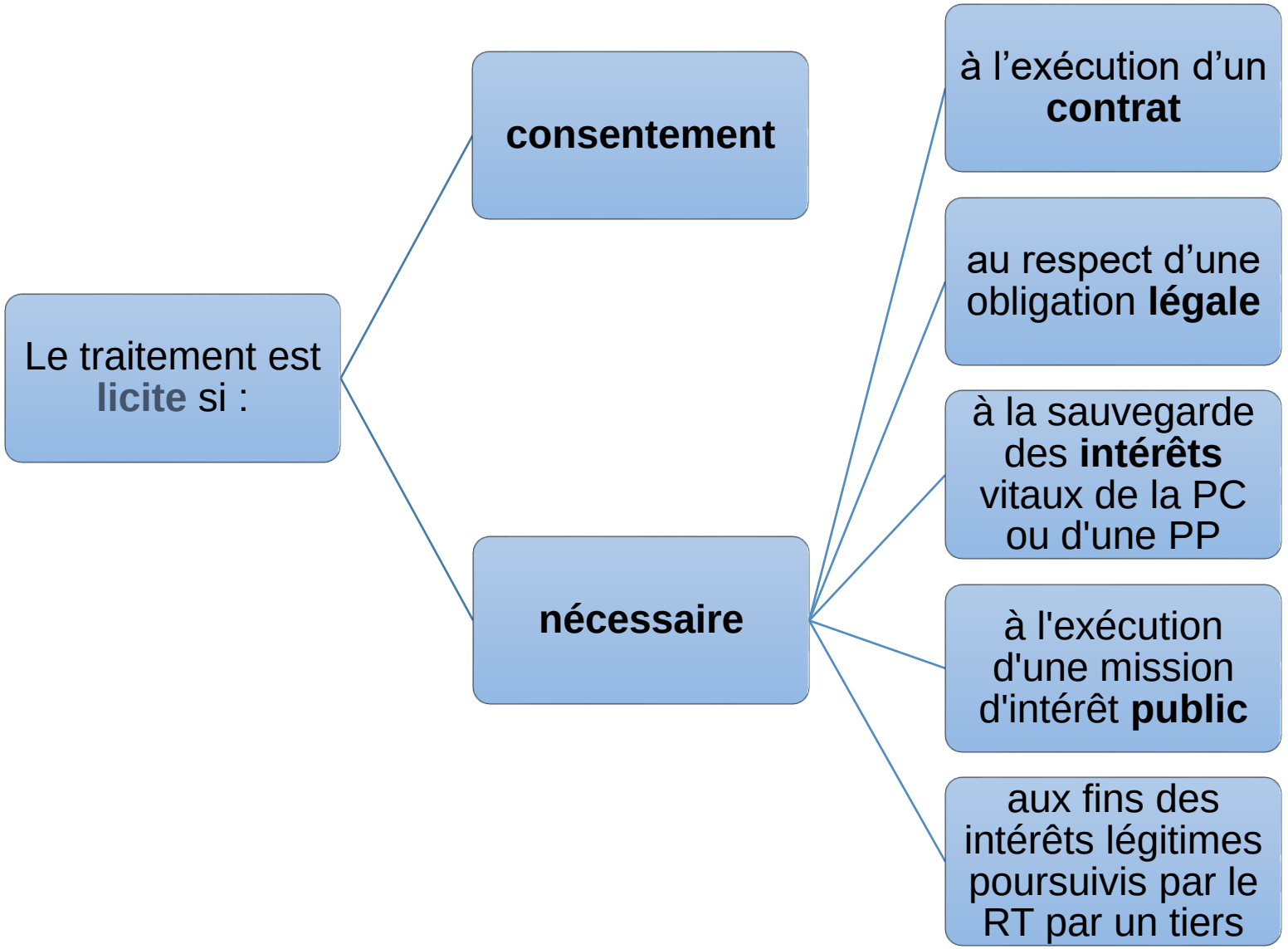
Principes généraux :

- traitées **loyalement**, **licitement** et de manière **transparente**
- dans une **finalité** déterminée, explicite, légitime

  (compatibilité du traitement ultérieur sauf cas particuliers)
- **minimisation** des données : adéquates, pertinentes et limitées à ce qui est nécessaire par rapport aux finalités
- **exactes** et si nécessaires, mises à jour
- conservées pour une **durée non excessive** par rapport au but poursuivi
- **intégrité** et **confidentialité**

→ Principe de responsabilité ou d'« **accountability** » : charge de la preuve RT

4. Licéité du traitement



5. Conditions applicables au consentement

Conditions renforcées

- une **action** positive et explicite >< implicite
- **démontrable** par le responsable du traitement (écrit, termes clairs et simples, forme compréhensible aisément accessible)
- **retrait** du consentement à tout moment
- **informer** clairement la personne concernée de cette possibilité
- **liberté** du consentement

+ règles **particulières** :

- les **enfants** âgés de moins de 16/13 ans
- les données **sensibles**
- les données **judiciaires**

6. Catégories particulières de données

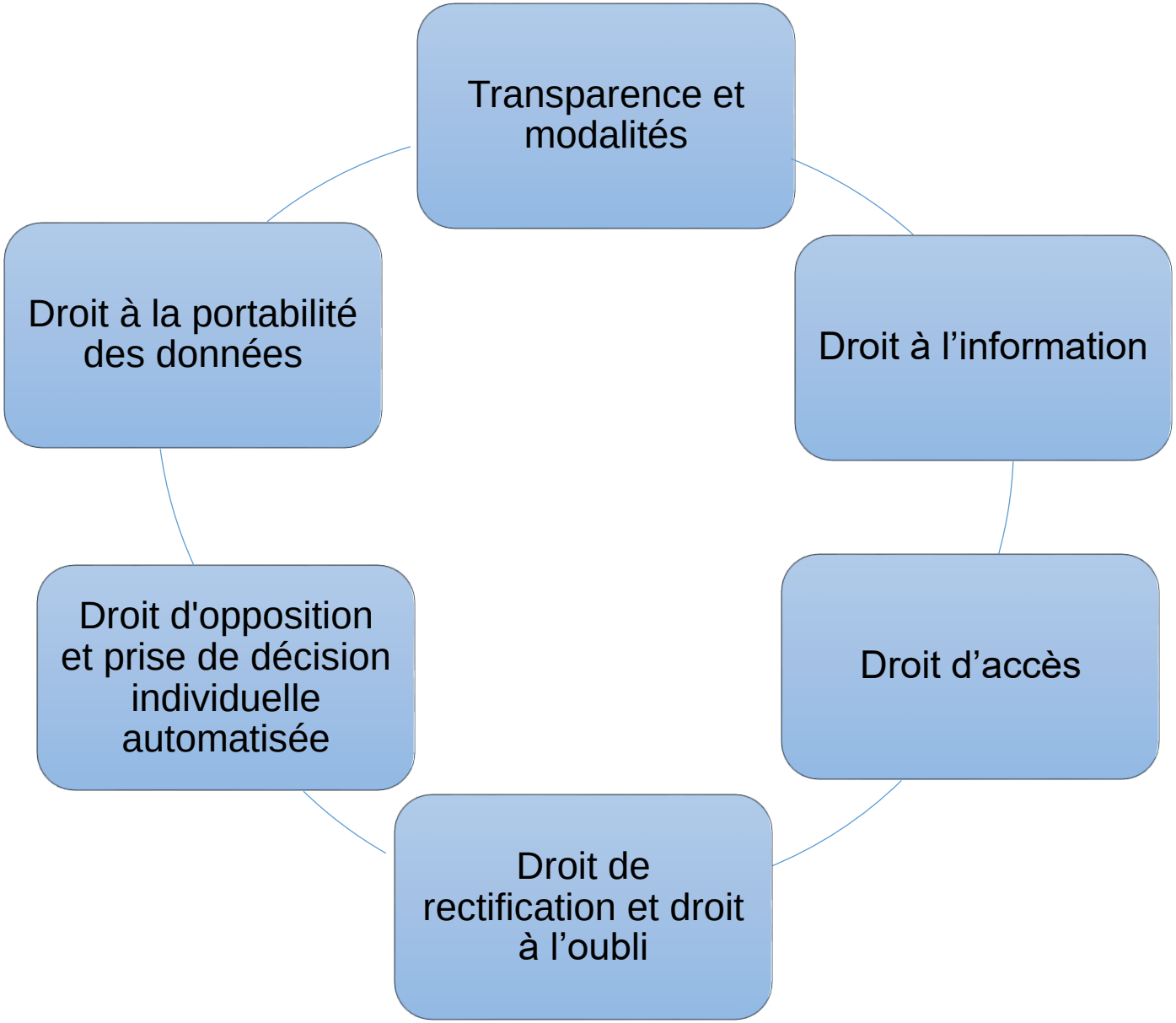
Principe : interdiction (données de santé, origine raciale, politique, ect.)

Exceptions :

- **consentement** explicite >< interdiction légale
- **nécessaire** en droit social (CCT – sécurité sociale)
- **intérêts vitaux**
- **ASBL**, recherches scientifiques, archivistes
- **données** manifestement rendues **publiques** par l'intéressé
- motifs d'**intérêts publics** dans un rapport de proportionnalité
- **autres** prévues par le droit national

+ règles **particulières** les **enfants** âgés de moins de 16 ans

7. Droits de la personne concernée



7. 1. Transparence et modalités

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Principes

- **mesures appropriées** pour la communication (ex : par écrit ou voie électronique/oralement sur demande)
- d'une **façon** concise, transparente, compréhensible et aisément accessible, en des termes **clairs et simples,**
- en particulier pour toute information destinée spécifiquement à un **enfant**
- au **moment de la collecte** ou dans un **délai raisonnable**

+ Le RT facilite l'exercice des droits et fournit les informations sur les mesures prises dans les **meilleurs délais** et en tout état de cause, dans un **délai d'un mois**

7. 2. Droit à l'information

Au moment de la **collecte** des données, le RT fournit :

- l'identité et les coordonnées du **responsable** du traitement
- les coordonnées du **délégué** à la protection des données
- catégories de **destinataires**
- Les **finalités** et bases de **licéité** du traitement
- le cas échéant, les **intérêts légitimes** du responsable du traitement
- l'information relative au **transfert** des données

+ Le RT **notifie** à chaque destinataires des données tout **rectification, effacement ou limitation** du traitement sur base des articles 16, 17 §1 et 18 **sauf s'il** démontre qu'une telle communication se révèle impossible ou suppose des **efforts disproportionnés**

7. 2. Droit à l'information

Informations complémentaires afin de garantir **équité** et **transparence**

- la durée de **conservation** ou les critères
- l'existence des **droits** d'accès, de rectification, d'effacement, de limitation, de portabilité, d'opposition
- la possibilité de **retirer** le consentement à tout moment si le traitement est fondé sur celui-ci
- le droit de **réclamation** auprès de la CPVP
- la collecte et à son **refus** (obligation règlementaire ou contractuelle)
- l'existence d'une **prise de décision automatisée**, y compris un profilage

7. 3. Droit d'accès

Droit d'accès : obtenir la **confirmation** du traitement de DACP (ou pas)

→ **accès** et/ou **copie** (sous forme électronique)

+ droit aux **informations** suivantes :

- les **finalités** du traitement et les **catégories** de DAPC
- les **destinataires** ou catégories de destinataires auxquels les DACP ont été ou seront communiquées, en particulier les destinataires établis hors UE
- la **durée de conservation** si ce n'est pas possible, les **critères** utilisés pour la déterminer
- le droit d'introduire une **réclamation** auprès de la CPVP

Exception : le droit d'obtenir une copie ne peut pas affecter négativement les **droits et libertés d'autrui**

7. 4. Rectification et effacement

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Droit à la rectification

- dans les meilleurs délais, rectification des **DACP inexactes**
- + **complétudes** des données

Droit à « l'oubli » « dans les meilleurs délais » fondé sur l'un des **motifs** suivants

- DAPC ne sont plus **nécessaires** au regard des finalités
- **retrait du consentement** sur lequel est fondé le traitement, et absence d'autre fondement au traitement
- **opposition** au traitement et absence de motif légitime impérieux pour le traitement ou **droit spécifique d'opposition** en matière de marketing direct
- DACP ont fait l'objet **d'un traitement illicite**
- DACP doivent être effacées pour **respecter une obligation légale** du droit de l'UE/EM auquel le RT est soumis

7. 4. Rectification et effacement

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Modalités : obligation de moyen

Lorsque le RT a rendu **publiques** DACP, il prend des **mesures raisonnables** pour **informer** les RT qui traitent ces données que la personne concernée a demandé **l'effacement**, de procéder également au dit effacement de tout **lien** vers ces données, **copie** ou **reproduction** de celles-ci

Exceptions :

- le droit à la **liberté d'expression et d'information**
- le traitement de données à caractère personnel est prévu par la **loi**
- pour des **motifs d'intérêt public** dans le domaine de la santé publique
- à des fins **d'archivage** dans l'intérêt général ou à des fins **scientifiques**, **statistiques** et **historiques**
- à la constatation, à l'exercice ou à la défense **de droits en justice**

7. 5. Droit à la limitation du traitement

Droit à la limitation « dans les meilleurs délais » fondé sur l'un des **motifs** suivants :

- **l'exactitude** des DAPC est **contestée** (le temps nécessaire pour vérifier)
- DACP ne sont plus **nécessaires** à l'objectif poursuivi mais nécessaires à la personnes pour une **action en justice**
- DACP ont fait l'objet **d'un traitement illicite**
- pendant la vérification des motifs légitimes du **droit d'opposition**

7. 6. Droit à la portabilité des données

→ **Interopérabilité des données + leur transmission au nouveau RT**

« dans les meilleurs délais » / un mois, au besoin deux mois SI :

- le traitement est fondé sur le **consentement** ou sur un **contrat**
- effectué à l'aide de procédés **automatisés** >< manuel
- la transmission directe est **techniquement** possible

→ obligation de vérifier la pertinence des données reçues

Exception : ce droit ne s'applique pas au traitement **nécessaire à l'exécution d'une mission d'intérêt public** ou relevant de **l'exercice de l'autorité publique** dont est investi le responsable du traitement

→ Recommandation du Groupe Article 29 (voir ici)

7. 7. Droit d'opposition et prise de décision individuelle et automatisée

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Droit d'opposition

Droit de s'opposer à tout moment, pour des raisons tenant à **sa situation particulière**, à un traitement de DACP :

- pour la réalisation d'une mission d'intérêt public
- pour la défense de ses intérêts légitimes

Exception : le responsable du traitement 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

7. 7. Droit d'opposition et prise de décision individuelle et automatisée

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Décision individuelle automatisée

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

Exception :

- **autorisée** par le droit de l'UE/EM auquel le RT est soumis et qui prévoit également **des mesures appropriées** pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée
- la décision est fondée sur le **consentement** explicite de la personne concernée

7. 8. Limitations

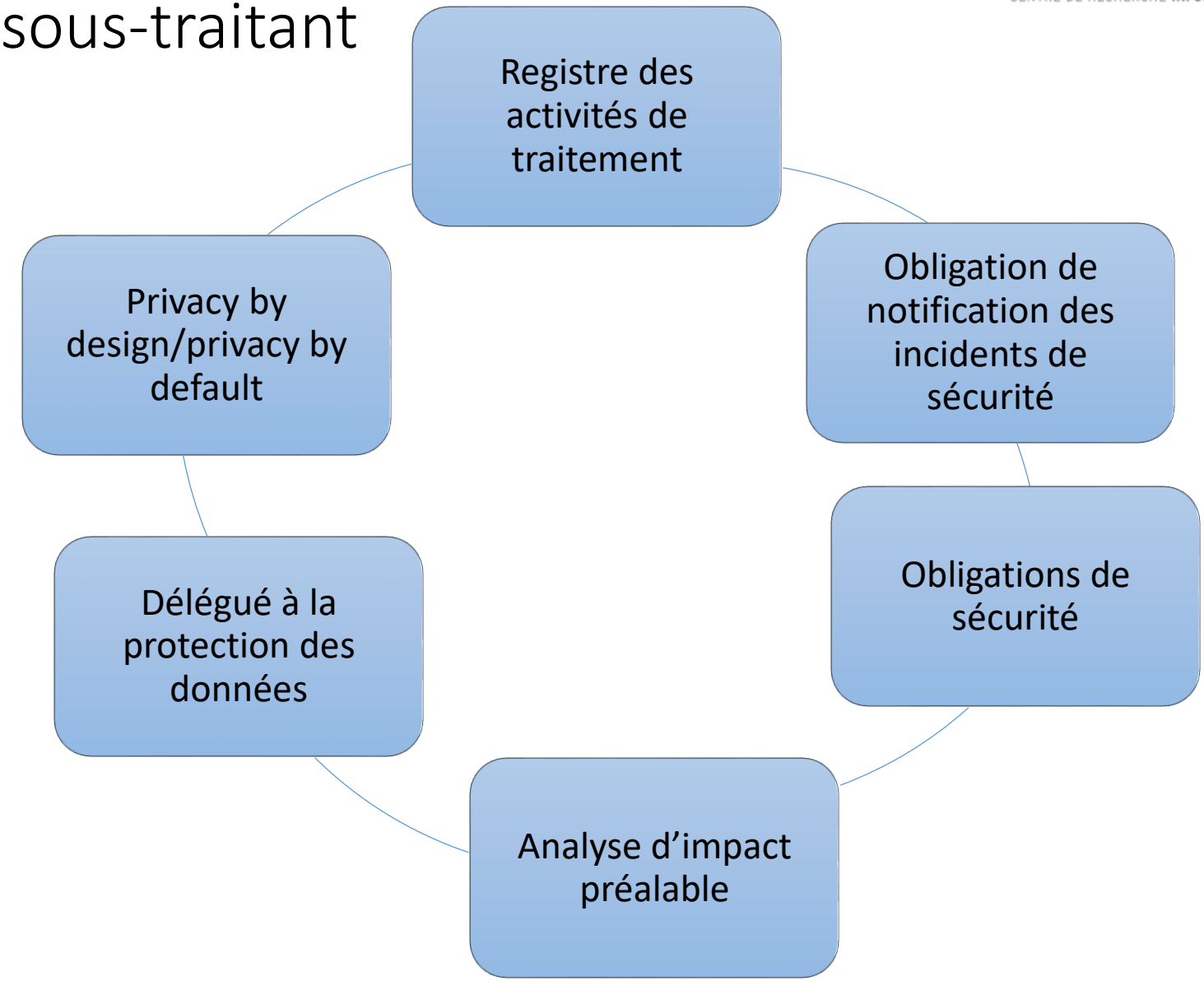
Limitation des droits de la personne concernés par **voie légale** si :

- cette limitation respecte **l'essence** des libertés et droits fondamentaux et qu'elle constitue une mesure **nécessaire** et **proportionnée** dans une société démocratique

- **pour garantir** notamment la sécurité nationale, la prévention et la détection des infractions pénales (…) ou d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ou encore pour l'exécution des demandes de droit civil

→ marge de manœuvre des EM importante >< objectif d'harmonisation

8. Obligations du responsable du traitement et du sous-traitant



8. Obligations du responsable du traitement et du sous-traitant

Principes généraux

- **choix** : ST présentant des **garanties suffisantes** quant à la mise en œuvre de **mesures** techniques et organisationnelles appropriées pour réponde aux exigences du GDPR et garantisse la protection des droits de la personne concernée

- **contrat**, comprenant notamment les éléments suivants :
    - les **finalités** du traitement de données
    - le **type** de données à caractère personnel
    - les **catégories** de personnes concernées
    - la **protection** adéquate des données
    - l'exécution **d'audits**
    - la **destruction** ou la **remise** des données à l'issue du traitement

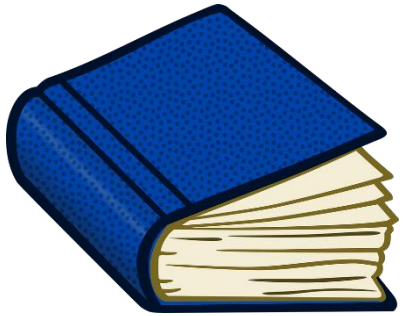
8.1. Le registre des activités de traitement

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

entreprises de plus de 250 employés

traitement susceptible de comporter un **risque** pour les droits/libertés des personnes concernées, s'il n'est **pas occasionnel**

ou s'il porte sur des catégories particulières de **données sensibles** ou relatives à des condamnations **pénales** et à des infractions



8.1. Le registre des activités de traitement

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Contenu du registre :

- Le **nom et les coordonnées** du responsable du traitement, du responsable conjoint, de son représentant et du délégué à la protection des données
- Les **finalités** du traitement
- Les **catégories** de **personnes** concernées et les catégories de **DACP**
- Les catégories de **destinataires**
- Les **transferts** de données vers un pays tiers
- Les **délais** prévus pour l'effacement
- Une **description** générale des **mesures** de sécurité techniques et organisationnelles

\+ pour **le ST** **: registre** de toutes les catégories d'activités de traitement effectuées pour le compte du RT

8.2. Obligations de sécurité renforcée

Mesures techniques et organisationnelles appropriées → garantir un niveau de sécurité **adapté au risque** compte tenu de:

- **l'état** des connaissances;
- des **coûts** de mise en œuvre;
- la nature, la portée, le **contexte** et les finalités du traitement;
- ainsi que les **risques**, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques.

→ Risque réel et potentiel!

8.2. Obligations de sécurité renforcée

Selon les **besoins**,

en ayant recours à

- la **pseudonymisation** et le **chiffrement** des DACP
- des **moyens** permettant de garantir la **confidentialité, l'intégrité, la disponibilité et la résilience constantes** des systèmes et des services de traitement
- des moyens permettant de **rétablir la disponibilité** des DACP et **l'accès** à celles-ci dans des délais appropriés en cas d'incident physique ou technique

8.2. Obligations de sécurité renforcée

Pseudonymisation:

- ***Art. 4, § 4, GDPR:*** *« le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise* ***sans avoir recours à des informations supplémentaires****, pour autant que ces informations supplémentaires* ***soient conservées séparément*** *et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »*

- ***Considérant 26 RGPD****: « Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation* ***et/****, qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable ».*

8.2. Obligations de sécurité renforcée

L'obligation de sécurité selon la CPVP:

•Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel (lien)

•Lignes directrices pour la sécurité de l'information (lien)

•Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données (lien)

La CPVP recommande déjà:

•La présence d'un conseiller en sécurité (en fonction de la nature des données)

•L'organisation et aspects humains de la sécurité de l'information

•La sécurité physique et de la sécurisation des réseaux

•La sécurisation logique des accès et la **journalisation, traçage et analyse des accès**

•La surveillance, revue et maintenance (audits)

•La gestion des incidents de sécurité et de la continuité

•De disposer d'une documentation

8.3. Analyse d'impact préalable

Obligatoire si:

- traitement susceptible d'engendrer un **risque** élevé pour les droits et libertés des personnes physiques + consultation préalable **CPVP**
- **évaluation systématique** et approfondie d'aspects personnels (**profilage)**
- le traitement **à grande échelle de données sensibles**
- **la surveillance systématique** à grande échelle d'une zone accessible au public.

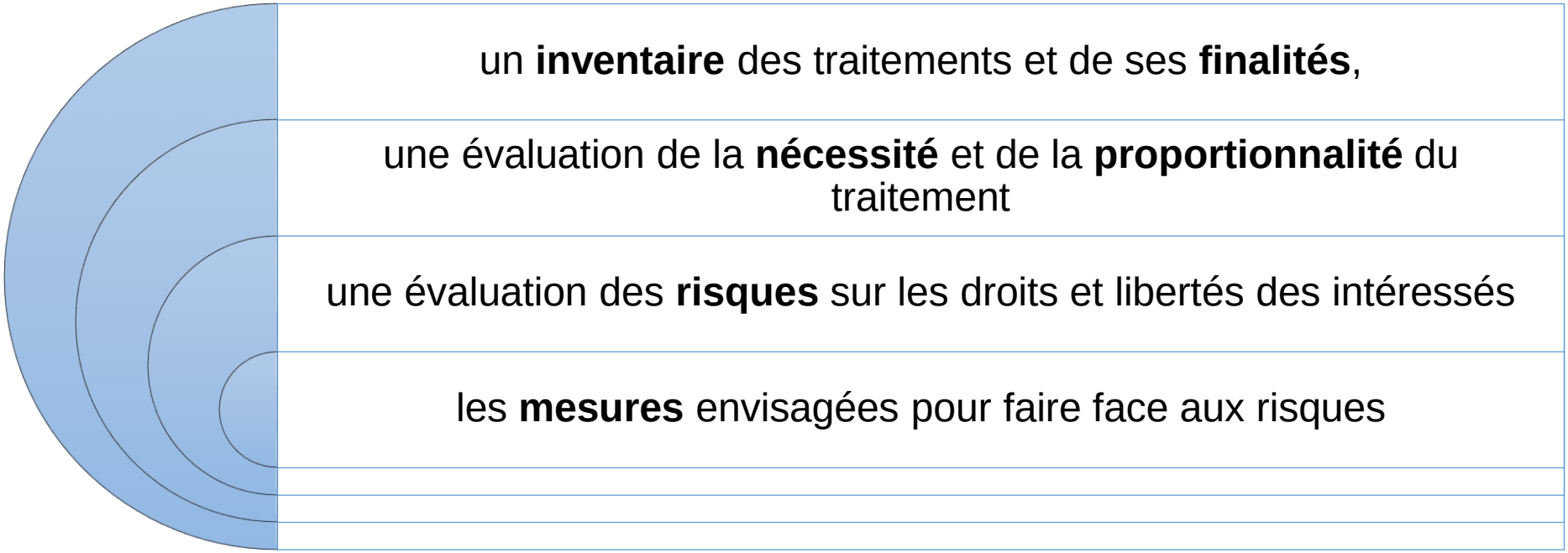
>< traitement justifié par le respect d'une obligation légale

>< médecin individuel, autre professionnel des soins ou par un avocat

>< sur base d'une liste établie par la CPVP

8.3. Analyse d'impact préalable

L'analyse d'impact **contient** au moins:



→ Recommandation du Groupe article 29 (ici)
→ Recommandation de la CPVP (ici)

8.4. Obligation de notification à la CPVP

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Procédure

- notification effectuée par le **RT**
- dans les **meilleurs délais**, si possible 72h à partir de la connaissance
  sinon après 72h, nécessité de motiver le retard
- **ST** doit notifier sans-délais au RT

Sauf si pas de **risque** pour les droits et libertés des personnes physiques

Quoi ?

- nature de la violation des données
- catégories-nombres de personnes/enregistrement concernés
- nom et des coordonnées du délégués à la protection des données
- description des conséquences probables
- description des mesures prises/à prendre afin de minimiser les aspects négatifs

8.4. Obligation de notification à la CPVP

CPVP
Commission de la protection de la vie privée

Plan du site • Lexique • FAQ • Presse • Liens • Contact •

THÈMES DE VIE PRIVÉE
Nos activités quotidiennes

LÉGISLATION ET NORMES
Textes de référence relatifs à la protection des données

DÉCISIONS
Nos avis, autorisations et recommandations

PUBLICATION
Les publications de Commission vie pri

Accueil > La notification de fuites de données

La notification de fuites de données

Lorsque des données à caractère personnel ont involontairement été piratées, volées ou rendues publiques d'une façon ou d'une autre, en premier lieu il est nécessaire d'en informer les personnes concernées.

S'il s'agit d'une fuite de données dans le secteur telecom ("violation"), il existe en outre une obligation légale de la notifier auprès de l'IBPT et de la Commission vie privée. Dans d'autres secteurs, il est opportun de notifier la fuite de données auprès de la Commission vie privée.

NOTIFICATION D'UNE FUITE DE DONNÉES DANS LE SECTEUR TELECOM

NOTIFICATION D'UNE FUITE DE DONNÉES DANS UN AUTRE SECTEUR

8.4. Obligation de notification à la PP

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Procédure

- effectuée par le **RT**
- **« dans les meilleurs délais »**
- si susceptible d'engendrer **un risque élevé** pour les droits et libertés d'une PP

Sauf dans trois situations constatées par la CPVP :

- **mesures de protection techniques et organisationnelles appropriées** ont été appliquées → données incompréhensibles (ex : chiffrement)
- **mesures ultérieures** qui garantissent que le risque élevé n'est plus susceptible de se matérialiser
- exigerait des **efforts disproportionnés** → communication publique

8. 5. Délégué à la protection des données

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Obligatoire pour :

- Les **organismes publics**
- Les entreprises dont les **activités de base** 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
    - les organisations qui traitent des "données sensibles" à grande échelle
    - dans les cas déterminés par un Etat membre

8. 5. Délégué à la protection des données

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Missions ?

- **informer et conseiller** sur les **obligations** en matière de protection des données et dispenser des **conseils**, sur demande, en ce qui concerne la « **PIA** » et vérifier l'exécution de celle-ci
- **accompagner et contrôler** le respect des dispositions matière de protection des données

  (la répartition des responsabilités, action de sensibilisation et la formation du personnel participant aux opérations de traitement, et réaliser les inventaires des traitements de données)
- **coopérer** être le point de **contact** de l'autorité de contrôle (**CPVP)**

8. 5. Délégué à la protection des données

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Quel DPO ?

- désigné sur la base de ses **qualités professionnelles** (droit et des pratiques en matière de protection des données) et de sa **capacité** à accomplir les missions qui lui sont confiées.
- disposer des **ressources nécessaires** pour exercer ces missions, ainsi que l'accès aux DACP et à leur traitement.
- **indépendance** : ne reçoit aucune instruction en ce qui concerne l'exercice des missions, il peut exécuter d'autres missions et tâches si celles-ci n'entraînent pas de conflit d'intérêts.
- soumis au **secret professionnel** ou à une obligation de confidentialité.

→ recommendation du **Groupe Article 29** **(ici)**

8. 6. Privacy by design/by default

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Privacy by design

Mise en œuvre de mesures techniques et organisationnelles pour une protection efficace des données (telles que la pseudo-anonymisation) tant lors de la définition des moyens de traitement que lors du traitement proprement dit

Privacy by default

Mise en œuvre de mesures techniques et organisationnelles pour limiter les traitements aux seules données personnelles nécessaires à la finalité

9. Divers : codes conduites/certifications

Les **codes de conduite**

- élaborés par les associations et entités représentant des RDT/ST
- doivent être soumis à la CPVP et approuvés par celle-ci.

Les **certifications** délivrés par des organismes de certification agréés :

- par la CPVP
- par BELAC (l'organisme d'accréditation belge)

→ peuvent servir d'élément pour démontrer le respect des exigences de sécurité

9. Divers : sanctions

- **Responsabilité civile** : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi

- **Responsabilité administrative :** augmentation du montant des amendes « administratives » : 20,000,000 EUR ou 4% du chiffre d'affaires annuel global réalisé par l'entreprise (le + élevé est retenu)

- **Responsabilité pénale :** compétence EM

Conclusions

Merci pour votre attention !

Franck Dumortier

Centre de recherche information, droit et société (CRIDS)

Université de Namur

Franck.dumortier@unamur.be

www.crids.eu

CENTRE DE RECHERCHE **INFORMATION, DROIT ET SOCIÉTÉ**