

# Le RGPD

## Des principes à la pratique

Luxembourg  
7 mars 2018

Christophe BUSCHMANN  
Membre Effectif



# Introduction

## Objectifs pour cette séance

### Sensibiliser – Réalité vs. mythe

- Vous guider pour que vous puissiez avancer de manière constructive

### Priorisation - Les éléments essentiels

- Identifier les éléments les plus pertinents - priorisation

### Pragmatisme - Cas pratiques

- Approche pratique qui ne focalise pas sur les exceptions exotiques mais plutôt les cas de tous les jours

## Agenda

### Éléments clés

- Définitions
- Principes

### Cas pratiques

- Fichier client
- Recrutement
- ...

# Introduction

## Guidance

### WP29-Validée

- DPO
- Portabilité
- DPIA
- Décisions automatisées et le profilage
- Notifications des violations de données
- ...

### WP29-En cours de validation:

- Consentement
- Transparence

### WP29-En consultation publique

- Dérogations pour les transferts
- Accréditation

### En cours / à venir:

- Obligations du registre des traitements pour PME
- Droit à l'oubli (mise à jour)
- Certification

### Commission Européenne

- Guidance - section dédiée

## Récentes évolutions

### Data breach

- Publication d'une section dédiée
- Email et formulaire de notification (sur base volontaire)

### Cours / formations

- Workshops pratiques pour faciliter l'utilisation de l'outil CST
- Suite des cours d'introduction à la protection des données

### DPO

- Publication d'une section dédiée avec formulaire de désignation (en cours)

### DPIA

- Publication d'une section dédiée avec formulaire pour consultation obligatoire (en cours)

### Brochures

- Obligations des entreprises
- Droits des personnes concernées

# Agenda

## Eléments clés

- Définitions
- Principes

## Cas pratiques

- Fichier client
- Recrutement
- ...

# Définitions

Données à caractère personnel

Traitement

Registre des activités de traitement (\*)

Responsable de traitement / Sous-traitant

DPO – Délégué à la protection des données (\*)

Autorité de contrôle



(\*) Le RGPD prévoit des dispositions spécifiques qui peuvent notamment s'appliquer aux petites structures pour lesquelles le traitement de données à caractère personnel ne constitue pas le cœur de métier.

# Données à caractère personnel



Toute information  
liée à une personne  
physique

**RGPD:** toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» 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

## **Exemples:**

- **Données en clair:** les données permettant l'identification immédiate d'une personne: **nom, prénom de vos clients,....**
- **Les données pseudonymisées :** possibilité d'identifier une personne moyennant un effort de recherche plus ou moins important: **numéro client, numéro de facture, adresse IP**



**Les données anonymisées ne sont pas/plus des données personnelles:** impossibilité totale d'établir un lien avec une personne physique: -> Le règlement ne s'applique pas. Évaluez la possibilité de travailler avec des données anonymisées.

# Traitement



**Toute manipulation  
sur base de ou  
impliquant des  
données  
personnelles**

**RGPD:** 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, telles que 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

**Exemples:**

- Recrutement, Ressources humaines, Fichier fournisseur, fichier clients, prospection... (cf. sections suivantes)



**Niveau de détail / granularité:** La description/ définition d'un traitement peut être faite à différents niveaux de détail. Si la décision du niveau de détail nécessaire revient à l'entreprise concernée - il est possible d'adopter une approche modulaire regroupant sous un libellé plusieurs « traitements » (p.ex. e libellé « ressources humaines » peut comprendre le recrutement, la gestion des carrières, la gestion des salaires,...)

# Responsable de traitement



L'organisation qui prend les décisions de ce qui est collecté et ou fait avec les données

**RGPD:** 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; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre

## Exemples:

- Vous êtes typiquement responsable de traitement pour tout ce que vous faites pour votre compte: **Gestion des salaires, gestion des fichiers clients et fournisseur, Prospection**,... (ces activités peuvent être sous-traités à une autre organisation – mais VOUS êtes le resp. de traitement)



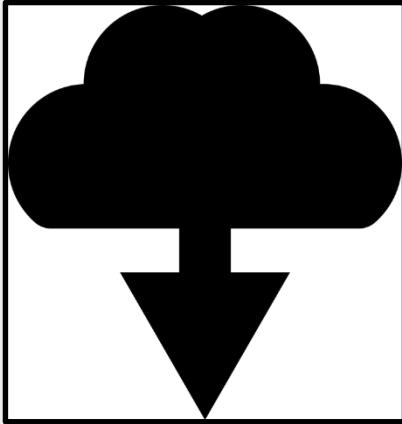
**Obligations:** Pour chaque traitement il doit y avoir obligatoirement (au moins) un responsable de traitement. Vous n'êtes typiquement pas responsable de traitement pour tout traitement que vous faites exclusivement sur instruction d'un de vos clients et qui implique des données personnelles – il est recommandé de vérifier cette interprétation avec eux en cas de doute.



**Transferts de données:** Pour les traitements qui sont effectués par les autorités publiques sur base de données que vous leurs transmettez vous n'est pas le responsable de traitement. Mais vérifiez si vous avez le droit / l'obligation de fournir les données.



# Sous-traitant



L'organisation qui  
traite des données  
pour vous

**RGPD:** 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.

## Exemples:

- Fiduciaire (gestion des salaires)
- Fournisseur IT (gestion d'une newsletter, hébergement de vos données,.....)
- Agence de recrutement (gestion des demandes)

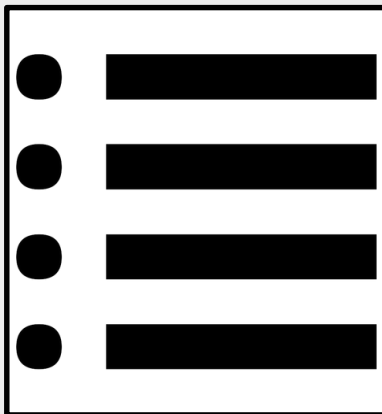


**Obligations:** Vous êtes responsable du traitement – il appartient à vous de ne pas demander des traitements qui ne sont pas conformes à la loi. Même si le sous-traitant peut voir doit vous aider – la décision et responsabilité reste avec vous.



**Contrat:** Le nouveau règlement exige qu'un certain nombre de clauses par rapport à la protection des données doivent figurer dans les contrats. Si votre sous-traitant ne vous a pas déjà contacté il peut être opportun de vérifier le contrat et le cas échéant le contacter pour le mettre à jour. Ceci serait aussi une bonne occasion pour le cas échéant clarifier les traitements qui sont effectués.

# Registre des activités de traitement



Un document/fichier  
qui reprend la  
description de  
l'ensemble de vos  
traitements

**RGPD:** Registre qui, pour chaque activité de traitement, comporte notamment les informations suivantes:

- a) le nom et les coordonnées du responsable du traitement (...)
- 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 (...)
- e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale(...)
- 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 organisationnelles (...)

## **Exemples:**

- « Compliance Support Tool » de la CNPD, CPVP, CNIL



**PME:** Pour les entreprises de moins de 250 entreprises, qui ne sont pas engagés sur des traitements à risque, pour qui les traitement ne sont qu'occasionnels et ne portent pas due des catégories particulières de données - la tenue d'un registre n'est pas obligatoire. Dans ces cas un registre peut néanmoins vous aider dans votre évaluation de conformité. Attention – une clarification de l'article 29 sur ce point est en cours d'élaboration. (Press release 02/2018)

**Réutilisation:** Le règlement n'est pas prescriptif quant à la forme du registre. Alors que les exemples ci-dessus peuvent vous aider à construire un registre nous vous recommandons de produire un registre qui est cohérent avec votre organisation – en terme de forme et vocabulaire utilisé.

# Registre – quelques exemples

Fiche de registre		ref-000
Description du traitement		
Nom / sigle		
N° / REF	ref-000	
Date de création		
Mise à jour		
Acteurs		
Nom	CP	Ville
Pays	Tel	
Responsable du traitement		
Délégué à la protection des données		
Représentant		
Responsable(s) conjoint(s)		
Finalité(s) du traitement effectué		
Finalité principale		
Sous-finalité 1		
Sous-finalité 2		
Sous-finalité 3		
Sous-finalité 4		
Sous-finalité 5		
Mesures de sécurité		
Mesures de sécurité techniques		
Mesures de sécurité organisationnelles		
Catégories de données personnelles concernées		
Etat civil, identité, données d'identification, images...		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation financière, données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM, etc.)		

**Illustratif**

@ CNIL

Vous trouverez dans cet onglet quelques listes qui pourront vous aider à compléter le registre.

Vous trouverez dans cet onglet quelques listes qui pourront vous aider à compléter le registre. Ces listes sont indicatives, tant en ce qui concerne le niveau de détail que l'exhaustivité. Il incombe au responsable du traitement d'indiquer au besoin des informations plus détaillées au sujet du traitement. Cliquez sur le '+' à côté du nom d'une liste pour l'ouvrir.

**Illustratif**

Liste indicative de types de finalités

Fondement du traitement

Liste indicative des catégories de données fonctionnelles

type de traitement

catégorie de données RGPD

liste indicative de catégorie(s) de destinataires

nature de la transmission vers un pays tiers/une organisation internationale

@ CPVP



GDPR-CST

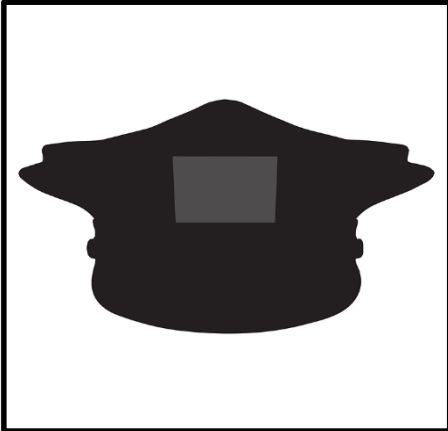
Registre des activités de traitement

Partie 2: Traitements	Partie 2: Tra	Partie 2: Tra
<p>Title: <b>Contract management</b></p> <p>Creat. on: 18 July 2017    Updat. on: 05 October 2017 Creat. by: Paul Richard    Updat. by: Paul Richard</p> <p>Draft</p>	<p>Title: <b>Analyse</b></p> <p>Creat. on: 18 July 2017    Updat. on: 05 October 2017 Creat. by: Paul Richard    Updat. by: Paul Richard</p> <p>Draft</p>	<p>Title: <b>invoicing</b></p> <p>Creat. on: 08 August 2017    Updat. on: 05 October 2017 Creat. by: Paul Richard    Updat. by: Paul Richard</p> <p>Draft</p>
<p>Title: <b>Payroll</b></p> <p>Creat. on: 05 October 2017    Updat. on: 05 October 2017 Creat. by: Paul Richard    Updat. by: Paul Richard</p> <p>Draft</p>	<p>Title: <b>Maintenance</b></p> <p>Creat. on: 06 October 2017    Updat. on: 06 October 2017 Creat. by: Paul Richard    Updat. by: Paul Richard</p> <p>Draft</p>	<p>Title: <b>Infrastructure</b></p> <p>Creat. on: 06 October 2017    Updat. on: 06 October 2017 Creat. by: Paul Richard    Updat. by: Paul Richard</p> <p>Draft</p>

**Illustratif**

@ CNPD & LIST

# Délégué à la protection des données



« Pilote » qui aide le responsable dans sa mise en conformité

**RGPD:** 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.

**Activité de base:** tous les organismes exercent certaines activités comme la rémunération de leurs employés ou les activités d'assistance informatique classiques. Ces activités constituent des exemples de fonctions de soutien nécessaires à l'activité de base ou principale de l'organisme. Bien que ces activités soient nécessaires ou essentielles, elles sont généralement considérées comme des fonctions auxiliaires plutôt que comme l'activité de base.

**PME:** Il est recommandé d'analyser au cas par cas leur situation individuelle. Il est possible, voir probable que de nombreuses PME n'ont pas d'obligation pour désigner une DPO.



# Autorité de contrôle



**Autorité qui assure la bonne application des règles en termes de protection es données**

**RGPD:** autorité publique indépendante chargée de surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union

## **Exemples de nos missions:**

- Sensibiliser et guider les entreprises et le public
- Gérer les plaintes de personnes concernées
- Effectuer des contrôles
- Conseiller le parlement / le gouvernement
- ...

**National:** Au Luxembourg l'autorité de contrôle est la CNPD « Commission nationale pour la protection des données ». Plus d'informations sont disponibles sur notre site internet [www.cnpd.lu](http://www.cnpd.lu)

**Europe:** Dans chaque pays de l'Union Européenne il existe une autorité de contrôle (i.e. l'équivalent de la CNPD). En France il s'agit de la CNIL, en Belgique il s'agit du CPVP. Toutes les autorités de contrôle collaborent au niveau européen – ce groupe s'appelle « EDPB » European data protection board. La CNPD représente le Luxembourg dans ce groupe.

# Principes relatifs au traitement des données à caractère personnel

Licité , loyauté  
et transparence

Limitation des  
finalités

Minimisation  
des données

Exactitude des  
données

Durée de  
conservation

Intégrité et  
confidentialité

**Responsabilisation**

# Licité, loyauté et transparence

**RGPD:** Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (**licéité, loyauté, transparence**)

**Licité:** Votre traitement doit remplir au moins UNE des 6 conditions suivantes (art.6):

	Condition	Exemples illustratifs
a)	Les personnes concernées vous ont donnée leur <b><u>consentement</u></b>	Envoi de courriers de publicité / newsletter
b)	Le traitement est <b><u>nécessaire</u></b> pour exécuter un <b><u>contrat</u></b>	Paieement des salaires
c)	Le traitement est <b><u>nécessaire</u></b> au respect d'une <b><u>obligation légale</u></b>	Transmission de données financières aux contributions directes
d)	Le traitement est <b><u>nécessaire</u></b> à la sauvegarde des <b><u>intérêts vitaux</u></b> de la personne concernée ou d'une autre personne physique;	Traitement dans un service d'urgences dans un hôpital
e)	Le traitement est <b><u>nécessaire</u></b> à l'exécution d'une <b><u>mission d'intérêt public</u></b>	Faire le remboursement de prescriptions médicales par la CNS
f)	Le traitement est nécessaire aux fins de vos <b><u>intérêts légitimes</u></b> poursuivis <b><u>SOUS CONDITION</u></b> qu'ils sont <b><u>plus important que ceux des personnes concernées</u></b>	Surveiller l'accès au trésor de d'entreprise



Le consentement doit être libre éclairé et univoque (art.7)



Probablement pas applicable pour vous



Nécessite une analyse et documentation plus détaillée

# Licité, loyauté et transparence

**RGPD:** Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (**licéité, loyauté, transparence**)

**Loyauté et transparence:** Vous devez informer les personnes concernées que vous traitez leurs données et comment vous le faites (art. 13 en cas de collecte directe et art. 14 en cas de collecte indirecte). Vous devez leur donner les informations suivantes

Information	Exemples illustratifs
<b><u>Vos coordonnées</u></b> – le cas échéant les coordonnées de votre délégué à la protection des données	Votre adresse email et ou postale, un numéro de téléphone,...
<b><u>La finalité</u></b> du traitement (i.e. pourquoi vous traitez leurs données)	Gestion des salaires, prospection,....
<b><u>La base juridique</u></b> de votre traitement (cf. comme évoqué toute à l'heure). Si la base est votre intérêt légitime – vous devez indiquer quels sont ces intérêts	Cf. voir page précédente
<b><u>Les destinataires</u></b> / catégories de destinataires s'ils existent	CNS, Contributions directes, agence marketing, fiduciaire,...
Votre éventuelle <b><u>intention de transférer leurs données à un pays tiers</u></b>	Système IT opéré aux Etats-Unis



D'autres informations peuvent être demandées – veuillez-vous référer aux articles 13 et 14



En cas de collecte indirecte vous devez informer l'origine des données (art. 14)



Vous devez donner ces informations lors de la collecte ou juste après – il appartient à vous de déterminer la meilleure forme



# Limitation des finalités

**RGPD:** Les données à caractère personnel doivent être collectées pour **des finalités déterminées, explicites et légitimes**, et **ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités**; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités)

Vous devez **définir de manière claire le but que vous cherchez à atteindre** par la traitement – et vous n'avez pas le droit pour utiliser les données pour autre chose.

Traitement	Finalité(s) – exemples illustratifs	
Vidéosurveillance	Sécurité des personnes	✓
	Protéger vos biens – éviter le vol	✓
Vidéosurveillance	Surveiller les personnes	✗ Pas explicite
Système de badges d'employés	Vérifier les horaires de travail	✓
Prospection	Envoyer des publicités aux personnes qui ont postulé pour être embauché au sein de mon entreprise	✗ Incompatible

# Minimisation des données

**RGPD:** Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

Vous ne devez pas collecter et/ou traiter des données qui ne sont pas nécessaires pour atteindre votre finalité – i.e. vous devez vous limiter à ce qui est NECESSAIRE et non pas à ce qui est UTILE.

Traitement	Finalité(s) – exemples illustratifs	Données nécessaires	Données utiles
Vidéosurveillance	Sécurité des personnes,	Images de la zone de la caisse (manipulation d'argent) ✓	Images de la zone « pause café » ✗
	Protéger vos biens – éviter le vol		
Gestion des ressources humaines	Versement des salaires	Coordonnées bancaires, Montant du salaire, montants versés les mois précédents, heures supplémentaires, statut marital ✓	Date de remboursement du prêt logement de la personne ✗
	Recruter une personnes	Nom, coordonnées de contact, expérience professionnelle ✓	Statu marital, nombre d'enfants ✗

# Exactitude des données

**RGPD:** Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude)



Je demande à mes clients une fois par an de vérifier si leurs coordonnées de contact et de facturations sont toujours à jours.



J'utilise un CV vieux de plus d'un an pour prendre une décision de recrutement.

# Durée de conservation

**RGPD:** Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en oeuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);



Un de mes employés a quitté mon entreprise. 3 ans après je supprime son dossier ressources humaines.



Je garde tous les CV des personnes ayant postulé pour une poste que j'ai déjà pourvu - on ne sais jamais à quoi cela peut servir.

# Intégrité et confidentialité

**RGPD:** Les données à caractère personnel doivent être traitées de façon à **garantir une sécurité appropriée** des données à caractère personnel, y compris la protection 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 ou organisationnelles appropriées (intégrité et confidentialité)

Vous ne devez pas mettre en place les mesures de sécurité nécessaires et proportionnelles au risque.

Traitement	Finalité(s) – exemples illustratifs	Mesures en place – exemples illustratifs
Vidéosurveillance	Sécurité des personnes,	L'accès au système pour visualiser les images est limité au strict minimum (p.ex. garde de sécurité), mon système journalise de qui a consulté les images, l'accès au système en dehors des locaux du bureau n'est pas possible,...
	Protéger vos biens – éviter le vol	
Gestion des ressources humaines	Versement des salaires	Le fichier qui contient les instructions pour la fiduciaire est protégé par mot de passe, les fiches de salaire sont fournis sous une enveloppée scellée avec mention « confidentiel et personnel »,...
	Recruter une personnes	Les CV sont enregistrés dans un répertoire ou seulement les personnes impliquées dans la procédure de recrutement ont accès,...

# Agenda

## Eléments clés

- Définitions
- Principes

## Cas pratiques

- Fichier client
- Recrutement
- ...

# Checklist simplifiée

**Objectif**: Fournir une **aide pragmatique** afin d'évaluer de manière simple votre niveau de **maturité par rapport à un traitement de données**



La checklist proposée se concentre sur les principes de la protection des données du RGPD (art. 5). Sans être exhaustive elle peut cependant constituer un outil pragmatique. Ainsi elle peut constituer un élément de début – pour les question plus approfondies nous proposons de se référer aux chapitres respectifs du RGPD.

# Checklist simplifiée

## Fiche signalétique

### Données traitées

- Enumérer les types de données traitées (p.ex. noms, adresses, certificats de maladie, comptables,...)

### Personnes concernées

- Enumérer les types personnes sur lesquelles porte le traitement (p.ex. clients, salariés, prospects, potentiels recrutés,...)

### Finalité du traitement

- Décrire l'objectif que le traitement permet d'atteindre (p.ex. paiement des salaires, envoi de factures, prospection de potentiels clients,...)

### Suppression

- Décrire si les données traitées sont nécessaires pour d'autres traitements respectivement des obligations légales

### Rôles et responsabilités

- Analysez si vous êtes l'entreprise qui décide ce qui est fait avec les données ou si vous êtes exécutant.
- Analysez si vous recevez ou transmettez les données à une autre organisation

## Questionnaire

	Questions	Remarque
1	Est-ce que j'ai le droit d'effectuer ce traitement?	<b>Principe: <u>licéité</u></b>
2	Est-ce que les personnes concernées sont au courant du traitement?	<b>Principe: <u>transparence</u></b>
3	Est-ce que j'utilise ces données pour faire autre chose / est-ce que j'utilise des données qui proviennent d'un autre traitement?	<b>Principe: <u>limitation des finalités</u></b>
4	Est-ce que toutes les données sont nécessaires – pas seulement utiles?	<b>Principe: <u>minimisation</u></b>
5	Est-ce que les données sont correctes et à jour?	<b>Principe: <u>exactitude</u></b>
6	Est-ce que je peux supprimer les données à la fin du traitement – ou est-ce qu'il y a une nécessité (pas une utilité) de les garder?	<b>Principe: <u>durée de conservation limitée</u></b>
7	Est-ce que les données sont sécurisées?	<b>Principe: <u>sécurité</u></b>



Cette fiche signalétique est inspirée des informations qui doivent figurer dans un « registre des activités de traitement » tel que défini dans l'article 30 du RGPD. Il ne s'agit ainsi d'un sous-ensemble des informations qui doivent être dans le registre.



Le questionnaire est inspiré des « principes relatifs au traitement de données à caractère personnel » tel que défini dans l'article 5 du RGPD.

# Cas pratique #1

## Le recrutement



### Fiche signalétique

### Questionnaire

#### Données traitées

- Nom, prénom, adresse postale, email, numéro de téléphone, qualification des candidats, ~~numéro de sécurité sociale~~ (\*)

#### Personnes concernées

- Potentiels recrutés (personnes physiques)

#### Finalité du traitement

- Embaucher un nouveau vendeur

#### Suppression

- A priori, après le recrutement

#### Rôles et responsabilités

- Mon entreprise est responsable de traitement

#### Questions

#### Réponse (O/N)

1. Est-ce que j'ai le droit d'effectuer ce traitement? Est-ce que chaque finalité est légale?	Oui -précontractuel
2. Est-ce que les personnes concernées sont au courant du traitement?	Oui – annonce
3. Est-ce que j'utilise ces données pour faire autre chose / est-ce que j'utilise des données qui proviennent d'un autre traitement?	Oui – personne sélectionnée Non – candidats non retenus
4. Est-ce que toutes les données sont nécessaires – pas seulement utiles?	Non (*)
5. Est-ce que les données sont correctes et à jour?	Oui - confirmation à demander
6. Est-ce que je peux supprimer les données à la fin du traitement – ou est-ce qu'il y a une nécessité (pas une utilité) de les garder?	Cf. question 3
7. Est-ce que les données sont sécurisées et confidentielles?	Oui - Répertoire avec accès limités,...



# Cas pratique #2

## Les ressources humaines



### Fiche signalétique

#### Données traitées

- Nom, prénom, adresse, téléphone, situation familiale, coordonnées bancaires, numéro de sécurité sociale, fiches de salaire, contrat etc..

#### Personnes concernées

- Salariés

#### Finalité du traitement

- Paiement du salaire, déclarations sociales/fiscales

#### Suppression

- 3 ans après fin de contrat de travail (délai de recours)
- Fiches de salaires (10 ans)

#### Rôles et responsabilités

- Mon entreprise est responsable du traitement
- Transfert à fiduciaire (sous-traitant)
- Transfert administration (fiscales, sociales, etc...)

### Questionnaire

Questions	Réponse (O/N)
1. Est-ce que j'ai le droit d'effectuer ce traitement? Est-ce que chaque finalité est légale?	Oui – exécution d'un contrat, obligation légale
2. Est-ce que les personnes concernées sont au courant du traitement?	Oui - contrat
3. Est-ce que j'utilise ces données pour faire autre chose / est-ce que j'utilise des données qui proviennent d'un autre traitement?	Oui – provenance de certaines données du recrutement
4. Est-ce que toutes les données sont nécessaires – pas seulement utiles?	Oui
5. Est-ce que les données sont correctes et à jour?	Oui, sous réserve que les salariés notifient les changements - vérifier.
6. Est-ce que je peux supprimer les données à la fin du traitement – ou est-ce qu'il y a une nécessité (pas une utilité) de les garder?	Conservation pour obligation légale
7. Est-ce que les données sont sécurisées et confidentielles?	Oui – répertoire avec accès limité Back up,...

# Cas pratique #3

## Le fichier fournisseurs



### Fiche signalétique

#### Données traitées

- Nom de l'entreprise, adresse du fournisseur;
- **Coordonnées de la personne de contact; statut marital de la personne de contact (\*\*);**
- Coordonnées bancaires \*

#### Personnes concernées

- Staff du fournisseur

#### Finalité du traitement

- Passer et suivre des commandes, paiement des factures.

#### Suppression

- A la fin de la relation commerciale avec fournisseur
- 10 ans pour les preuves de transactions commerciales (factures)

#### Rôles et responsabilités

- Mon entreprise est responsable du traitement

\* Les données d'identification de l'entreprise ne sont pas des données personnelles

### Questionnaire

Questions	Réponse (O/N)
1. Est-ce que j'ai le droit d'effectuer ce traitement? Est-ce que chaque finalité est légale?	Oui – exécution d'un contrat/ commande
2. Est-ce que les personnes concernées sont au courant du traitement?	Oui - commande
3. Est-ce que j'utilise ces données pour faire autre chose / est-ce que j'utilise des données qui proviennent d'un autre traitement?	Non
4. Est-ce que toutes les données sont nécessaires – pas seulement utiles?	Non (**)
5. Est-ce que les données sont correctes et à jour?	Oui, sous réserve d'une mise à jour régulière.
6. Est-ce que je peux supprimer les données à la fin du traitement – ou est-ce qu'il y a une nécessité (pas une utilité) de les garder?	Conservation pour obligation légale
7. Est-ce que les données sont sécurisées et confidentielles?	Oui – répertoire avec accès limité,...

# Cas pratique #4

## Le fichier clients



### Fiche signalétique

#### Données traitées

- Nom, prénom, adresse, Coordonnées bancaires? Habitude d'achat?

#### Personnes concernées

- Client (particuliers ou personne de contact d'une entreprise)

#### Finalité du traitement

- carte fidélité, suivi/exécution commande

#### Suppression

- Carte fidélité -> selon le consentement
- Preuves comptables à conserver 10 ans

#### Rôles et responsabilités

- Mon entreprise est responsable du traitement
- Utilisation d'un logiciel X (local)

### Questionnaire

Questions	Réponse (O/N)
1. Est-ce que j'ai le droit d'effectuer ce traitement? Est-ce que chaque finalité est légale?	Oui – contrat Consentement
2. Est-ce que les personnes concernées sont au courant du traitement?	Oui - contrat
3. Est-ce que j'utilise ces données pour faire autre chose / est-ce que j'utilise des données qui proviennent d'un autre traitement?	Non
4. Est-ce que toutes les données sont nécessaires – pas seulement utiles?	Peut-être
5. Est-ce que les données sont correctes et à jour?	Oui, sous réserve d'une mise à jour régulière.
6. Est-ce que je peux supprimer les données à la fin du traitement – ou est-ce qu'il y a une nécessité (pas une utilité) de les garder?	Conservation pour obligation légale
7. Est-ce que les données sont sécurisées et confidentielles?	Oui – répertoire avec accès limité,..

# Cas pratique #5

## Publicité (prospection)



### Fiche signalétique

#### Données traitées

- Nom, prénom, adresse, email, téléphone

#### Personnes concernées

- Clients ou Prospects

#### Finalité du traitement

- Proposer un produit/service à un client ou à tiers

#### Suppression

- Prospection: délai raisonnable (p.ex. délai pour prendre une décision)
- Client: cf fichier client

#### Rôles et responsabilités

- Mon entreprise est responsable du traitement

### Questionnaire

Questions	Réponse (O/N)
1. Est-ce que j'ai le droit d'effectuer ce traitement? Est-ce que chaque finalité est légale?	Oui - consentement
2. Est-ce que les personnes concernées sont au courant du traitement?	Oui – au moment du recueil du consentement
3. Est-ce que j'utilise ces données pour faire autre chose / est-ce que j'utilise des données qui proviennent d'un autre traitement?	Oui pour les clients – Non pour les prospect
4. Est-ce que toutes les données sont nécessaires – pas seulement utiles?	Oui
5. Est-ce que les données sont correctes et à jour?	Oui, sous réserve d'une mise à jour régulière.
6. Est-ce que je peux supprimer les données à la fin du traitement – ou est-ce qu'il y a une nécessité (pas une utilité) de les garder?	Oui – prospects Non - clients
7. Est-ce que les données sont sécurisées et confidentielles?	Oui – répertoire avec accès limité,...

# Commission nationale pour la protection des données

*Merci pour votre attention!*

