RGPD :
Protection des données à caractère personnel

I. Introduction

Plan

A. Qu’est ce qu’une donnée à caractère personnel ?
B. Pourquoi les utilise-t-on ?
C. Quels sont les risques de leur utilisation ?
D. Quels sont les textes qui encadrent leur utilisation ?

A. Qu’est ce qu’une donnée à caractère personnel

- «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable.
- Exemple : noms, prénoms, adresses, plaques d’immatriculation, photos, empreintes digitales ou génétiques, n° de sécurité sociale, n° de tél…

B. Pourquoi les utilise-t-on ?

- Les données sont utilisées dans de nombreux secteurs : marketing, intelligence artificielle, administration
- Toutes ces utilisations donnent de la valeur aux données. Du coup, elles se louent, se vendent, s'échangent. De nombreuses activités ont pour objectif de collecter des données (objets connectés, jeux ou services gratuits…)

C. Quels sont les risques de leur utilisation ?

- Des exemples de mauvaises utilisations avérées
  - Utilisation par le régime de Vichy du Numéro National Inscription au registre national d'identification
  - Registre Safari : naissance de la loi informatique et liberté
  - Cambridge Analytic
- On peut imaginer bien pire
  - la solution finale avec les données de géolocalisation
  - Affectation des enfants dans des études en fonction de leur « probabilité de réussite »…

D. Quels sont les textes qui encadrent leur utilisation ?

- Loi informatique et liberté du 06 janvier 1978 modifié par
  - la loi du 06 août 2004 -> création de la CNIL
  - la loi du 20 juin 2018
- Règlement général de protection des données (2016) qui remplace la directive de 1995

II. Philosophie du RGPD

Plan

A. Objectifs généraux
B. Les points clés du RGPD

A. Objectifs généraux

1) Sanctuariser les données à caractère personnel
2) Prendre en compte l'impact des nouvelles technologies
3) Renforcer la protection et la sécurité des données
4) Unifier les réglementation européenne

PLAN

1) Sanctuariser les données à caractère personnel

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental (inscrit dans la charte des droits fondamentaux européens au même titre que l'interdiction de l'esclavagisme ou le respect à l'intégrité physique et moral

2) Prendre en compte l’impact des nouvelles technologies

Le RGPD tient compte des évolutions des nouvelles technologies : profilage, objets connectés, géolocalisation, intelligence artificielle, marketing prédictif.

3) Renforcer la protection et la sécurité des données

La valeur des données entraîne une augmentation des attaques contre leurs propriétaires.

Le RGPD impose des règles de sécurisation

4) Unifier les réglementations européennes

a) Différence entre règlement et directive
b) Champ d'application

a) Différence entre règlement et directive

- Une directive fixe des objectifs à atteindre
- Un règlement s’applique directement

b) Champ d’application

- Le champ d’application matériel : tous les traitements de données à caractère personnel (sauf ceux effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique)
- Champ d’application territorial :
  - le responsable du traitement ou le sous-traitant à son établissement principal au sein de l’UE ou
  - les produits ou services ciblent l’ensemble des résidents européens

B. Les points clés du règlement

1) Accountability
2) Privacy by design, privacy by default
3) La transparence
4) La responsabilité du sous traitant
5) Le Délégué à la protection des données
6) Des sanctions dissuasives

PLAN

1) Accountability

Avant RGPD

- Déclaration des traitements avant leur réalisation

Après RGPD

- Principe d'accountability = capacité de prouver le respect de la réglementation
  - Mise en place de procédure documentée
  - Gestion d’un registre des traitement

2) Privacy by design, privacy by default

- Privacy by design : Il faut prévoir la sécurisation des données en amont du projet et tout mettre en œuvre pour les protéger
- Privacy by default : il faut limiter la collecte de données à ce qui est strictement nécessaire, les traiter avec précaution et limiter les personnes et organisation qui y ont accès.

3) La transparence

- Il faut indiquer aux personnes concernées de façon claire et intelligible quelle utilisation de leurs données il va être fait
- Il faut leur indiquer leurs différents droits
- En cas de violation des données personnelles les entreprises doivent prévenir la CNIL sous 72h voir informer les personnes concernées. Celles-ci peuvent demander réparation des préjudices matériels et moraux subis.

4) La responsabilité du sous traitant

Avant le RGPD, seul le responsable du traitement pouvait être sanctionné. Maintenant les sous-traitants sont aussi tenu comme responsable en cas de manquement.

5) Le délégué à la protection des données

- Le délégué à la protection des données est la personne qui sera l'interlocuteur de l'autorité de tutelle (CNIL).
- La nomination d'un DPO est obligatoire :

  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

  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 sensibles ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Comme le texte n'est pas très clair, il faut interpréter. Le groupe 29 a indiqué que les organismes suivants ont l'obligation de recruter un DPO :

E commerçant qui font du retargeting, entreprise qui exploitent un système de fidélité, les acteurs du secteur des objets connectés…

6) Des sanctions dissuasives

Le montant des sanctions augmentent avec le temps

- **Avant 2016** plafond de 150 000 € voir 300 000 € en cas de récidive
- **De octobre 2016 jusqu'à mai 2018** : plafond de 3 millions
- **Avec le RGPD** : jusqu'à 20 millions ou 4% du CA annuel mondial

III. **Définitions des notions clés**

Plan

A. Les données à caractère personnel
B. Les données sensibles
C. Les traitements
D. Le responsable du traitement et le sous-traitant
E. Le transfert hors union européenne

A. Les données à caractère personnel

«données à caractère personnel», 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; »

B. Les données sensibles

1) Définitions
2) Autorisation du traitement
3) Conséquence du traitement

PLAN

1) Définitions

Art 9 du RGPD interdit les traitements des données sensibles :

Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2) Autorisation du traitement

Ce même article liste 10 exceptions notamment :

- la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale
- le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée;

3) Conséquences du traitement

- L’article 35 du RGPD prévoit la conduite d’une analyse d’impact relative à la protection des données (AIPD - Data Protection Impact Assessment), lorsqu‘un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

C. Les traitements

«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, 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;

D. Le responsable du traitement et le sous-traitant

- «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; 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;
- «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;

E. Le transfert hors union européenne

Le transfert de données hors Union Européenne notamment aux états unis est très encadré.

Cependant ces transferts ne rentre pas dans le cadre de ce cours

IV. Collecter des données

Plan

- Etape 1 : Minimiser les données
- Etape 2 : Choisir la base juridique du traitement
- Etape 3 inscrire le traitement au registre des traitements
- Etape 4 : Informer les personnes

Etape 1 : Minimiser les données

1) Principes
2) Finalités
3) Durées de traitement

PLAN

1) Principes

- Les données à caractère personnel doivent être :
  - traitées de manière **licite, loyale et transparente** au regard de la personne concernée
  - collectées pour des **finalités déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalité
  - **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

2) Finalités

- La finalité est la raison d'être du traitement. Elle doit être indiquée à la personne concernée de façon claire, précise et simple.
- Les données récoltées doivent être en lien direct avec la finalité énoncée
- Il est interdit de modifier la finalité ultérieurement

3) Durées de traitement

- Il faut se fixer une durée de conservation des données qui doit être en lien avec la finalité. La CNIl en 2016 indiquait :
  - Données clients : 3 ans après le dernier échange commercial
  - Données prospect : 3 ans après le dernier contact (clic sur un lien contenu dans un mail. Par contre l'ouverture du mail n'est pas suffisant)

Etape 2 : Choisir la base juridique du traitement

- Les bases légales du traitement sont décrites dans l'art 6 du RGPD. Les principales sont
  - **L'exécution d'un contrat** souscrit entre le responsable de traitement et la personne concernée
  - **L'intérêt légitime du responsable de traitement**
  - **Le consentement de la personne concernée.**
  - Le traitement est nécessaire au respect d'une obligation légale pour le responsable du traitement
  - Sauvegarde d'intérêt vitaux
  - Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Etape 3 inscrire le traitement au registre des traitements

1) Contenu du registre
2) Qui doit tenir un registre

PLAN

1) Contenu du registre

- Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.
- Document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles et vous permet d'identifier précisément :
  - les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
  - les catégories de données traitées,
  - à quoi servent ces données (ce que vous en faites), qui accède aux données et à qui elles sont communiquées,
  - combien de temps vous les conservez,
  - comment elles sont sécurisées.

2) Qui doit tenir un registre

- Toutes les organisations sont concernées. Il existe une dérogation pour les entreprises de moins de 250 salariés qui doivent inscrire les seuls traitements suivants :
  - les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ;
  - les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.)
  - les traitements qui portent sur des données sensibles (exemple : données de santé, infractions, etc.).
- L'exception est donc très limitée car tous les traitements réguliers doivent apparaître.

Etape 4 : Informer les personnes

1) Principes
2) Quand faut il informer les personnes
3) Quelles sont les informations à donner ?

PLAN

1) Principes

- Quelle que soit la base légale de traitement, il est nécessaire d'informer les personnes concernées à l'aide de mentions obligatoires lors de la collecte d'informations directes ou indirectes (achetés, ou récupérés auprès d'un partenaires).
- Le RGPD précisent que ces mentions doivent être concises, transparentes, compréhensibles, et accessibles. Elles doivent être écrites dans un langage simple et clair.

2) Quand faut il informer les personnes

a) La distinction collecte directe et indirecte
b) Les exceptions à l'obligation d'informer

PLAN

a) La distinction collecte directe et indirecte

- En cas de collecte directe, les informations sont transmises lors du recueil des données.
- En cas de collecte indirectes, ces informations doivent être transmises dès que possible et au plus tard dans un délai de 1 mois.

b) Les exceptions à l’obligation d’informer

- la personne concernée dispose déjà de ces informations (il faut être capable de le prouver);
- la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés
- l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée;
- les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel.

3) Quelles sont les informations à donner ?

a) Principes
b) Les informations obligatoires ET prioritaires
c) Les informations obligatoires
d) Les informations qui dépendent du contexte

PLAN

a) Principes

- Le RGPD impose de fournir de nombreuses informations à la personne concernée « de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ».
- Il faut donc utiliser un vocabulaire simple et s'adapter au public visé (notamment les enfants). Il est nécessaire de prioriser l'information.
- Les informations prioritaires sont présentées sur les formulaires de collecte. Un lien est ajouté vers une notice d'information.
- Cette notice peut se présenter sous la forme de menus dépliants pour permettre à la fois une vue d'ensemble des données et un accès rapide à chaque information.

b) Les informations obligatoires ET prioritaires

- Identité du responsable de traitement
- Coordonnées du DPO si l'entreprise en a nommé un
- Finalité du traitement et la base juridique du traitement
- Caractère obligatoire ou facultatif des données qu'il collecte
- Existence des droit des personnes concernées :
  - Droit de s'opposer au traitement
  - Accès aux données
  - Rectification ou effacement des données
  - Droit à la portabilité des données
  - Introduire une réclamation auprès de la CNIL

c) Les informations obligatoires

- Durée de conservation des données
- Destinataires ou catégories de destinataires des données (qui a besoin d'y accéder ou de les recevoir au vu des finalités définies) ;
- Description des droits des personnes concernées :
  - Droit de s'opposer au traitement
  - Accès aux données
  - Rectification ou effacement des données
  - Droit à la portabilité des données
  - Introduire une réclamation auprès de la CNIL

d) Les informations qui dépendent du contexte

- Si transfert hors UE
  - existence d'un transfert des données vers un pays hors Union européenne (ou vers une organisation internationale) et garanties associées.
  - la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (exemples : clauses contractuelles types de la Commission européenne)
- l'existence d'une prise de décision automatisée ou d'un profilage, les informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que les conséquences pour la personne concernée
- Selon la base juridique :
  - le fait que les données sont requises par la réglementation,
  - le fait que les données sont requises par un contrat ou en vue de la conclusion d'un contrat ;
  - les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (exemple : prévention de la fraude) ;
  - le droit au retrait du consentement à tout moment (prioritaire) ;

V. Les droits des personnes

Plan

1) Le droit à l’information
2) Le droit d’opposition
3) Le droit d’accès aux données
4) Le droit de rectification
5) Le droit d’effacement
6) Le droit à la limitation du traitement
7) Le droit de portabilité
8) Décision individuelle automatisée et droit à une intervention humaine

1) Le droit à l’information

Voir étape 4 diapo 44

2) Le droit d’opposition

a) Principes
b) Exceptions
c) Cas de la prospection
d) Information

PLAN

a) Principe

Art 21 du RGPD 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.

- le traitement est 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
- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers

b) Exceptions

Le responsable du traitement pourra justifier son refus au motif que :

- il existe des motifs légitimes et impérieux à traiter les données ou que celles-ci sont nécessaires à la constatation, l'exercice ou défense de droits en justice ;
- la personne concernée a consenti au traitement – elle doit alors retirer ce consentement et non s'y opposer ;
- un contrat lie la personne à l'organisme ;
- une obligation légale impose le traitement des données ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

c) Cas de la prospection

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.

d) Information

Au plus tard au moment de la première communication avec la personne concernée, le droit visé aux paragraphes 1 et 2 est explicitement porté à l'attention de la personne concernée et est **présenté clairement et séparément de toute autre information**.

3) Le droit d’accès aux données

Art 15 du RGPD La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations fournies lors de la collecte.

4) Le droit de rectification

- Art 16 du RGPD 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.
- Si le responsable du traitement rectifie des données, il doit prévenir la personne concernée à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

5) Le droit d’effacement

a) Principe
b) Motifs d’application

PLAN

a) Principe

- Dans certaines situations, Art 17 du RGPD indique que la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant.
- Dans le cas où le responsable de traitement efface des données, il doit en notifier la personne concernée.

b) Motifs d’application

- le responsable du traitement a l'obligation d'effacer ces données à caractère personnel lorsque l'un des motifs suivants s'applique:
  - les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;
  - la personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement;
  - la personne concernée s'oppose au traitement
    - en vertu de l'article 21, paragraphe 1 (opposition à des traitement basé sur le consentement), et il n'existe pas de motif légitime impérieux pour le traitement,
    - en vertu de l'article 21, paragraphe 2 (opposition à une prospection);
  - les données à caractère personnel ont fait l'objet d'un traitement illicite;
  - les données à caractère personnel 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
  - les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1 (enfants).

6) Le droit à la limitation du traitement

a) Principe
b) Motifs d'application
c) Exemples d'utilisation
d) Réutilisation des données
e) Notification de la personne concernée

PLAN

a) Principe

La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement. Cela signifie qu’aucun traitement ne doit être effectué sur les données à par la conservation.

Les données sont « gelées »

b) Motifs d’application

- Motifs d’application
  - 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; ou
  - le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation; ou
  - 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; ou
  - la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1 (opposition à des traitement basé sur le consentement), 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.

c) Exemples d'utilisation

- Soit la personne concernée s'oppose à un traitement et demande au responsable du traitement de geler l'utilisation des données, le temps que celui-ci examine la demande (diffusion d'une image sur un réseau social)
- *Soit le responsable du traitement souhaite supprimer des données et la personne concernée demande leur gel (et donc leur conservation) le temps d'exercer un droit (les images de vidéo surveillance sont supprimées au bout d'un mois)*

d) Réutilisation des données

- Une fois gelées, les données ne peuvent être utilisées qu’avec le consentement de la personne concernée ou :
  - pour la constatation, l'exercice ou la défense de droits en justice,
  - pour la protection des droits d'une autre personne physique ou morale,
  - pour des motifs importants d'intérêt public de l'Union ou d'un État membre.

e) Notification de la personne concernée

Le responsable du traitement doit informer la personne concernée lorsqu'il limite un traitement et avant de lever cette limitation.

7) Le droit de portabilité

a) Principes
b) Transmission à un tiers
c) Droit et libertés des tiers

PLAN

a) Principe

- 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 :
  - la base juridique du traitement est le consentement ou la réalisation d'un contrat
  - le traitement est effectué à l'aide de procédés automatisés.

b) Transmission à un tiers

Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

c) Droit et libertés des tiers

Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés de tiers (par exemple si la personne qui exécute ce droit transmet des données permettant d'identifier d'autres personnes (un carnet d'adresse) le destinataire des données ne pourra pas utiliser ces données (pour faire de la prospection par exemple).

8) Décision individuelle automatisée et droit à une intervention humaine

a) Principes
b) Exceptions
c) Droits minimums
d) Usages de données sensibles

PLAN

a) Principes

Art 22 du RGPD : 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.

a) Principes

Art 22 du RGPD : 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.

b) Exceptions

- Ce droit ne s’applique pas lorsque la décision :

  a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;

  b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou

  c) est fondée sur le consentement explicite de la personne concernée.

c) Droits minimums

Si la décision est nécessaire à la conclusion d'un contrat ou si elle est fondée sur le consentement explicite de la personne concernée, le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, en conférant à la personne concernée les droits minimums suivants :

- d'être informé qu'une décision entièrement automatisée a été prise à votre encontre ;
- de demander à connaître la logique et les critères employés pour prendre la décision ;
- de contester la décision et d'exprimer votre point de vue ;
- de demander l'intervention d'un être humain qui puisse réexaminer la décision.

d) Usage de données sensibles

Enfin les décisions auxquelles on ne peut s’opposer ne peuvent être basées sur des données sensibles sauf si la personne concernée a donné son accord, ou si le traitement est nécessaire pour des motifs d’intérêt public important.