G2S group

LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Sensibilisation

23 Janvier 2017

Aïssatou Sarr

Sensibilité :

Référence :

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

SOMMAIRE

- Partie I: Quelques définitions
  - ✓ Qu'est-ce qu'une donnée à caractère personnel ?
  - ✓ Quelles sont les données interdites ?
  - ✓ Qu'est-ce qu'une donnée de santé ?
  - ✓ Qu'est-ce qu'un traitement de données à caractère personnel ?
  - ✓ Qu'est-ce qu'un Responsable de traitement ?
  - ✓ Qu'est-ce qu'un destinataire ?
  - ✓ Qu'est-ce qu'un sous-traitant?
- Partie II: La loi n° 78-17 du 6 janvier 1978 dite « loi Informatique et Libertés »
  - ✓ L'historique
  - ✓ Les grands principes
  - ✓ Les sanctions
- Partie III: Le Règlement Européen
  - ✓ Les grands principes de la protection des données réaffirmés
  - ✓ Les ajouts du Règlement
  - ✓ Le renforcement des sanctions

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

SOMMAIRE

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

PARTIE I: QUELQUES DEFINITIONS

- Qu'est-ce qu'une donnée à caractère personnel ?

  - Article 4-1 du Règlement Général sur la Protection des Données (RGPD), (art 2-2 de al LIL)
  - Constitue une donnée à caractère personnel toute information relative à une **personne physique** identifiée ou qui peut être identifiée, **directement** ou **indirectement**, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
    - Par exemple: Nom, Prénom, date de naissance, adresse mail professionnelle, géolocalisation…

  - Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le Responsable du Traitement ou toute autre personne.
    - Par exemple: Si je sais qu'un homme politique a eu un scandale concernant des croissants, un scooter et une actrice:
      - Je peux en déduire que l'on parle de Mr François Hollande

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

Quelles sont les données interdites ?

- Article 9 du RGPD (art 8 de la LIL)
- Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement:
  - Les origines raciales ou ethniques
  - Les opinions politiques, les convictions religieuses ou philosophiques
  - L'appartenance syndicale
  - le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé
  - des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

- Les exceptions:
  - Dans le cas ou la personne donne son consentement explicite
  - Lorsque les traitements sont nécessaires à la sauvegarde de la vie humaine
  - Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice
  - Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la **gestion de services de santé** et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal
  - Etc…

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

Qu'est-ce qu'une donnée de santé ?

- Définition légale de la données de santé (article 4-15 du RGPD)
  - ✓ Les données concernant la santé sont les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.
  - ✓ Le RGPD précise dans le Considérant 35: que les données à caractère personnel concernant la santé devraient comprendre:
    - ✓ l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur.
    - ✓ Cela comprend des informations sur la personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services;
    - ✓ un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé;
    - ✓ des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques;
    - ✓ et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro.

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

Qu'est-ce qu'un traitement de données à caractère personnel ?

- Article 4- 1 du RGPD (2-3 de la LIL)
- 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
  - La modification
  - L'extraction
  - La consultation
  - L'utilisation
  - La communication par transmission
  - La diffusion ou toute autre forme de mise à disposition
  - Le rapprochement
  - L'interconnexion
  - La limitation
  - L'effacement
  - La destruction

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

- Qu'est-ce qu'un Responsable de traitement ?
  - Article 4-7 du RGPD (3-I de la LIL)
  - Un Responsable de Traitement (RT) est, 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

- Qu'est-ce qu'un destinataire ?
  - Article 4-9 du RGPD (3-II de la LIL)
  - Le destinataire d'un traitement de données est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données caractère personnel, qu'il s'agisse ou non d'un tiers

- Qu'est-ce qu'un sous-traitant ?
  - Article 4-8 du RGPD (35 de la LIL)
  - Le sous-traitant est 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;

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

PARTIE II: LA LOI INFORMATIQUE ET LIBERTÉS

- L'Historique

  - Le projet intitulé SAFARI, initié en 1973 qui avait pour but de croiser tout ou partie des fichiers administratifs français par le ministère de l'intérieur, à été révélé en 1974 par un article du Monde.

  - Ce qui a créé un scandale qui déboucha en 1978 sur l'adoption de la loi informatique et libertés.

  - Avec le développement du numérique, l'utilité de cette loi n'a fait que de se renforcer.

  - Toutefois, l'évolution de la société commence à mettre en évidence les limites de la loi, c'est pour cela qu'elle sera bientôt supplanté par un Règlement Européen

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

Les Grands principes de la loi

Principe de finalité

- Usage déterminé
- Usage légitime
- Tout détournement de finalité est passible de sanctions pénales

Principe de proportionnalité

- Doivent être utilisée des informations pertinentes
- Doivent être utilisée des informations nécessaires à la finalité du traitement

Principe de pertinence des données

- Les données doivent être adéquates
- Les données doivent être pertinentes
- Les données ne doivent pas être excessives

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

Principe de durée limitée de conservation des données

- Une durée de conservation doit être établie en fonction de la finalité de chaque traitement
- Le droit à l'oubli
  - La purge des données
  - L'archivage
  - L'anonymisation

Principe de sécurité et de confidentialité

- Obligation d'habilitation précise
- Les données ne doivent pas être déformées, endommagées ou que des tiers non autorisés y aient accès
- Mesures de sécurité physique et logique obligatoire
- Les mesures de sécurité doivent être adaptées à la nature des données et aux risques

Principe de transparence

- Les personnes concernées par le traitement doivent en être informées au préalable

Principe du respect du droit des personnes

- Droit d'accès
- Droit de rectification
- Droit d'opposition pour motif légitime

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

❑ Les Sanctions

- ✓ Un avertissement qui peut être rendu public
- ✓ Une sanction pécuniaire
- ✓ Une injonction de cesser le traitement
- ✓ Un retrait de l'autorisation accordée par la CNIL

En cas d'urgence et d'atteinte aux droits et libertés:

- ✓ L'interruption de mettre en œuvre le traitement
- ✓ L'avertissement
- ✓ Le verrouillage des données pour trois mois
- ✓ L'information au Premier Ministre afin qu'il prenne les mesures nécessaires

En cas d'atteinte grave et immédiate aux droits et libertés:

- ✓ La CNIL peut demander des référés aux juridictions compétentes
- ✓ La CNIL peut dénoncer au Procureur de la République les infractions

Depuis la loi du 29 mars 2011 les sanctions pécuniaires peuvent être rendue publique
Sans qu'il y ait besoin que l'organisme soit de mauvaise foi

Sanction Pénale: 5 ans d'emprisonnement et 300 000 euros d'amende

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

PARTIE III: LE REGLEMENT EUROPEEN

- Les grands principes de la protection des données réaffirmés

  - Principe de **licéité**
  - Principe de **loyauté**
  - Principe de **transparence** des traitements
  - Principe de **détermination** des finalités des traitements
  - Principe de **minimisation** et d'exactitude des données
  - Principe de **conservation limitée** des données (droit à l'oubli)
  - Principe de **sécurité** des données
  - Principe de **consentement** de la personne concernée renforcé
  - La tenue d'un **Registre** de donnée à caractère personnel

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

Les Grands Ajouts du Règlement

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

- Application du Règlement aux entreprises hors UE qui offre des biens ou des services à des personnes au sein de UE
- Ces entreprises doivent désigner un Délégué à la protection des données (ex CIL)
- Principe d'accountability
- Application du « Privacy by Design » (prise en compte des principes de protection des données personnelles dès la conception des projets)
- Application du « Privacy by Default » (prise en compte des principes de protection des données personnelles par défaut)
- Obligation de faire des Etudes d'Impact sur la Vie privée et des Analyses de risques
- Obligation de notifier les violations de sécurité des données personnelles
- Résilience constante des systèmes et des services de traitement
- Obligation d'avoir un Délégué à la protection des données (DPO ex CIL) rattaché directement au Responsable de Traitement, pour les entreprises de plus de 250 salariés, qu' elles soient Responsable de traitement ou sous traitant
- Renforcement des obligations des sous-traitants
- Responsabilité conjointe de traitement organisée (renforcement du principe de Co-responsable de traitement)
- Renforcement des droits des personnes
- Consécration de nouveaux droits (droit à la portabilité des données, droit à l'oubli, droit à la limitation des traitements
- Renforcement des certifications (BCR, Label CNIL)

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

❑ Le renforcement des sanctions

- Les sanctions financières peuvent aller jusqu'à **4% du chiffre d'affaires annuel mondial total de l'exercice précédent du groupe ou 20 000 000 d'euros** (art 79 du Règlement)

  Motifs:

  - ➢ non respect des principes de la protection des données
  - ➢ Infractions aux règles applicables au consentement
  - ➢ Infractions aux dispositions relatives aux transferts de données hors de l'EEE

- Les sanctions financières peuvent aller jusqu'à **2% du chiffre d'affaires annuel mondial total de l'exercice précédent du groupe ou 10 000 000 d'euros** (art 79 du Règlement)

  Motifs:

  - ➢ Absence de protection des données dès la conception et par défaut
  - ➢ Défaut de sécurité des données
  - ➢ Absence de notification des violations de données
  - ➢ Absence de Registre des traitements
  - ➢ Non respect des règles de désignation du DPO

- 5 ans d'emprisonnement pour le Responsable de Traitement (ancienne sanction qui sera surement confirmé dès l'application du Règlement)

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

Il est énoncé dans l ’article 84 du règlement Européen:

- ✓ Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives.

- ✓ Il est donc probable que les anciennes sanctions de la CNIL perdurent:
  - Un avertissement ou une mise en demeure qui peuvent être rendu public
  - Une injonction de cesser le traitement
  - Un retrait de l’autorisation accordée par la CNIL
  - Un blocage des données durant 3 mois

En cas d’urgence et d’atteinte aux droits et libertés:

- L’interruption de mettre en œuvre le traitement
- L’avertissement
- Le verrouillage des données pour trois mois
- L’information au Premier Ministre afin qu’il prenne les mesures nécessaires

En cas d’atteinte grave et immédiate aux droits et libertés:

- La CNIL peut demander des référés aux juridictions compétentes
- La CNIL peut dénoncer au Procureur de la République les infractions

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

PARTIE IV: LE CORRESPONDANT INFORMATIQUE ET LIBERTES (CIL) ou DELEGUE A LA PROTECTION DES DONNEES (DPO)

- Sa création:
  - ✓ Le rôle du CIL est défini par le décret d'application du 20 octobre 2005 concernant la loi 78-17 du 6 janvier 1978 modifiée le 06 août 2004

- Ses missions:
  - ✓ Réduire les risques de contentieux contractuel, administratif, judiciaire et réputationnel
  - ✓ Conseiller l'organisme sur les nouvelles manières d'exploiter les données
  - ✓ Rassurer les personnes extérieures à l'organisme
  - ✓ Appliquer les principes de la protection des données
  - ✓ Dresser une liste des traitements de données personnelles
  - ✓ Assurer le respect des obligations prévues par la loi
  - ✓ Fournir une expertise sur les projets
  - ✓ Gérer les demandes issues du droits des personnes
  - ✓ Etablir un bilan annuel

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

- Le renforcement des missions issu de l'article 39 du Règlement Européen:
  - ✓ Le Règlement Européen modifie le nom du Correspondant Informatique et libertés (CIL), il devient le Délégué à la Protection des Données ou Data Protection Officer (DPO)
  - ✓ **informer et conseiller** le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;
  - ✓ **contrôler** le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;
  - ✓ **dispenser** des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35;
  - ✓ **coopérer** avec l'autorité de contrôle;
  - ✓ faire office de **point de contact** pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.

- Il est énoncé dans le Règlement Européen que ses missions sont le minimum que doit effectuer le DPO et que ces nouvelles missions se cumulent aux précédentes.

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

PARTIE V:
LES RELAIS A LA PROTECTION DES DONNEES (RPO)

- Création:
  - ✓ Pas de texte de loi qui créé les RPO
  - ✓ La CNIL préconise cependant, selon la taille de l'entreprise que des Relais soient mis en place pour diffuser au mieux les implications de la loi « Informatique et Libertés »
  - ✓ C'est l'un des critères pour l'obtention des BCR et du Label Gouvernance de la CNIL

- Missions:
  - ✓ **de transmettre au DPO toutes informations lui permettant d'identifier un traitement de données à caractère personnel**
  - ✓ **d'être un point d'encrage du DPO concernant les projets d'obtention du Label Gouvernance CNIL et des Binding Corporate Rules (BCR)**
  - ✓ d'informer le DPO sur les nouveaux projets pour se mettre en conformité avec la CNIL,
  - ✓ de veiller dans leur entourage immédiat au respect de la loi informatique et liberté,
  - ✓ de diffuser les bonnes pratiques en matière de protection des données à caractère personnel.

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

PARTIE VI:
LES OBJECTIFS DE G2S GROUP

- ✓ La mise en conformité
  - Audit des traitements
  - Refonte des traitements
  - Cartographie des traitements

- ✓ Les Binding Corporate Rules (BCR)
  - Les Binding Corporate Rules (ci-après BCR) désignent un **code de conduite interne** qui définit la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne.
  - Les BCR doivent être contraignantes et respectées **par toutes les entités du groupe, quel que soit leur pays d'implantation**, ainsi que par tous leurs **salariés.**
  - **19 critères d'obtention**

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

LES REGLES CONTRAIGNANTES D'ENTREPRISE (BCR)

- Qu'est-ce que les BCR ?
  - ✓ Les Binding Corporate Rules (ci-après BCR) désignent un code de conduite interne qui définit la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne.
  - ✓ Les BCR doivent être contraignantes et respectées par toutes les entités du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs salariés.
- Quel est leurs intérêts ?
  - ✓ Les BCR constituent une alternative aux Clauses Contractuelles Types puisqu'elles permettent d'assurer un niveau de protection suffisant aux données transférées hors de l'Union européenne. En ce sens, elles constituent également une alternative aux principes du Safe Harbor pour les transferts vers les Etats-Unis.
- Quels sont les avantages ?
  - ✓ Les BCR permettent...
    - d'être en conformité avec les principes de la directive européenne 95/46/CE et du RGPD;
    - d'uniformiser les pratiques relatives à la protection des données personnelles au sein d'un groupe. ;
    - de prévenir les risques inhérents aux transferts de données personnelles vers des pays tiers ;
    - d'éviter de conclure autant de contrats qu'il existe de transferts au sein d'un groupe ;
    - de communiquer sur la politique d'entreprise en matière de protection des données personnelles auprès de ses clients, partenaires et salariés et de leur assurer un niveau de protection satisfaisant lors des transferts de leurs données personnelles ;
    - de constituer un guide interne en matière de gestion des données personnelles ;
    - de placer la protection des données au rang des préoccupations éthiques du groupe.

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

APPLICATION DANS LE GROUPE

- Création d'une Politique de Protection des données Groupe.
- Mise en place d'un plan de formation annuel afin que tous les salariés du Groupe connaissent les bases de la protection des données.
- Audit des traitements de données à caractère personnel annuel de toutes les entités du Groupe.
- Présentation des engagements des BCR à l'ensemble des salariés du Groupe ainsi que les procédures qui en découlent.
- Création de nouvelles procédures:
  - ✓ Fiche Réflexe,
  - ✓ Procédure d'Audit des traitements de données à caractère personnel,
  - ✓ Procédure de Demande de modification d'un traitement,
  - ✓ Procédure de Gestion des notifications des violations de données,
  - ✓ Procédure de Gestion des plaintes et du droit à réparation pour violation des BCR,
  - ✓ Procédure de Gestion du droit des personnes concernées,
  - ✓ Procédure de Gestion en cas de contrôle des Autorités de protection des données, etc…

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

MERCI DE VOTRE ATTENTION

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.

Ce document est propriété de G2S Group, il est mis votre disposition à des fins informatives.

G2S Group - Copyright 2016

Tous droits réservés

Toute utilisation de présentations dont les contenus sont élaborés par almerys doit être soumise à demande auprès de

marketing@almerys.com

© G2S Group - Document à valeur non contractuelle. Propriété exclusive de G2S Group. Reproduction interdite.