Jeudi 23 mai 2019

Bird & Bird

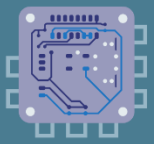
Cadre juridique : les points de vigilance du RGPD et le niveau de conformité des établissements

Merav Griguer
Avocat Associée

Points de vigilance identifiés

1. Remédiation et négociation des contrats
2. Analyses d'impact (PIA)
3. Violation de données à caractère personnel
4. Contrôles CNIL
5. Gouvernance DPO
6. *Accountability*
7. Formation et sensibilisation des salariés

ASSURANCES



SOCIÉTÉS DE GESTION

BANQUES

Bird & Bird

1. Remédiation et négociation de contrats (1/2)

Objectif : déterminer la qualification des parties

Responsable du traitement
Data Controller

Détermine les finalités et moyens du traitement

Obligations :
- Base légale du traitement
- Information des personnes concernées
- Respect des droits des personnes concernées
- Sécurité du traitement
- Réalisation des PIA obligatoires
- Notification des violations de données sources de risque

Sous-traitant
Data Processor

Réalise le traitement pour le compte et sur instructions du responsable du traitement

Obligations :
- Traitement pour le compte et sur instruction du responsable du traitement uniquement
- Assistance du responsable du traitement pour l'accomplissement de ses obligations
- Sécurité et confidentialité des données confiées ou collectées pour le compte du sous-traitant

⇒ Conséquences d'une mauvaise qualification :

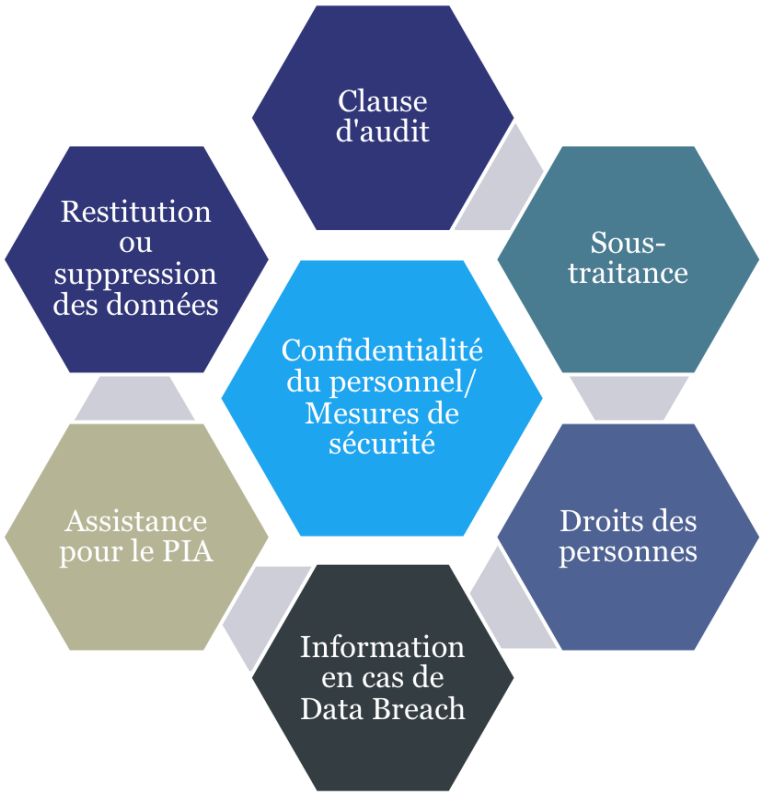
- Obligations des parties inadaptées
- Risque de sanction (ni la CNIL ni le juge ne sont liés par la qualification des parties)

Bird & Bird

1. Remédiation et négociation de contrats (2/2)

Négociation contractuelle

Article 28 du RGPD



Clauses bloquantes lors des négociations contractuelles :

- Sécurité et confidentialité des données :
  minima à respecter ? qui les définit ? détail de ces mesures ?
- Clause d'audit :
  délai d'information ? qualité de l'auditeur ?
- Clause de coopération :
  - violation de données : délai pour notifier ? format ? destinataires internes ?
  - droit des personnes concernées : qui réceptionne ? qui répond ? coût de l'assistance ?
- Clause de sous-traitance ultérieure : *possibilité de s'opposer à un sous-traitant ultérieur ? modalités ?*
- Clause de plafonnement de responsabilité : *clause spécifique de responsabilité "données personnelles" ? Plafond/déplafonnement ?*

Bird & Bird

2. Analyse d'impact (PIA)

PIA obligatoires et recommandés

PIA obligatoires :

Article 35 du RGPD: *"tout traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées"*

Publication d'une liste par la CNIL des traitements obligatoirement soumis à PIA,

Exemples:

- *"Traitements impliquant le profilage des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci;*
- *Traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle;*
- *Traitements de profilage faisant appel à des données provenant de sources externes."*

➢ Exemples dans le secteur bancaire et financier: traitements de *scoring*, profilage, décision automatisée.

PIA recommandés :

Exemples de critères du G29 :

- Evaluation ou notation *(incluant le profilage)*
- Prise de décision automatisée avec effet juridique ou effet similaire significatif
- Données sensibles ou données à caractère hautement personnel
- Traitement à grande échelle
- Croisement ou combinaison d'ensembles de données
- Utilisation d'innovation ou application de nouvelles technologies
- Traitement susceptible de priver les personnes de l'exercice d'un droit ou du bénéfice d'un service ou d'un contrat

→ Si un critère rempli **: PIA recommandé**
→ Si deux critères remplis **: PIA obligatoire**

Exemple de PIA recommandé dans le secteur bancaire et financier : hébergement des données bancaires des clients

Bird & Bird

3.Violation de données à caractère personnel

Détection, gestion et notification

Notification à la CNIL :

"Violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données"

- Qui ? Par le responsable de traitement.
- Quand ? Dans les meilleurs délais, et si possible sous 72h au plus tard après en avoir pris connaissance (retard à justifier).
- Obligation de documenter toute violation de données afin de permettre à la CNIL de contrôler a posteriori

Communication aux personnes concernées:

- Si la violation de données est "*susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique*", à moins que :
  - Des mesures de protection techniques et organisationnelles appropriées ont été prises ; ou
  - Des mesures ultérieures garantissent que le risque élevé n'est plus susceptible de se reproduire ; ou
  - La communication à personne nécessiterait des efforts disproportionnés (dans ce cas : communication publique ou mesure similaire).
- Quand ? Dans les meilleurs délais, dès que ce risque élevé est identifié, ou après injonction de la CNIL.

Bird & Bird

4. Contrôles CNIL (1/2)

Typologies de contrôles

- Contrôle en ligne
  - Effectué depuis les locaux de la CNIL
  - Sans la présence du responsable du traitement
  - Information du responsable par un procès-verbal de constatations en ligne

  ⇒ Les agents de la CNIL peuvent utiliser une **identité d'emprunt**.

- Contrôle sur pièces
  - Communication de documents sur demande écrite de la CNIL

- Contrôle sur audition
  - Convocation du responsable du traitement dans les locaux de la CNIL

- Contrôle sur place
  - Par les agents de la CNIL, dans les locaux du responsable du traitement

➢ ***Devoir de collaboration***

Attention: délit d'entrave

Bird & Bird

4. Contrôles CNIL (2/2)

Exemples de sanctions (avant RGPD)

banque et assurance

Avertissement public

Motif : manquement à l'obligation de mise à jour des données.

BNP PARIBAS

Avertissement public

Motif : manquement à l'obligation de mise à jour des données.

20.000 €

Motif : inscription abusive dans les fichiers de la Banque de France.

LCL BANQUE ET ASSURANCE

45.000 €

Motif : entrave à l'action de la CNIL et inscription abusive sur les fichiers de la Banque de France.

Banque des Antilles Françaises

30.000 €

Motif : inscription abusive dans les fichiers de la Banque de France.

Bird & Bird

Sanctions européennes

Exemple de sanction (post RGPD) - Allemagne

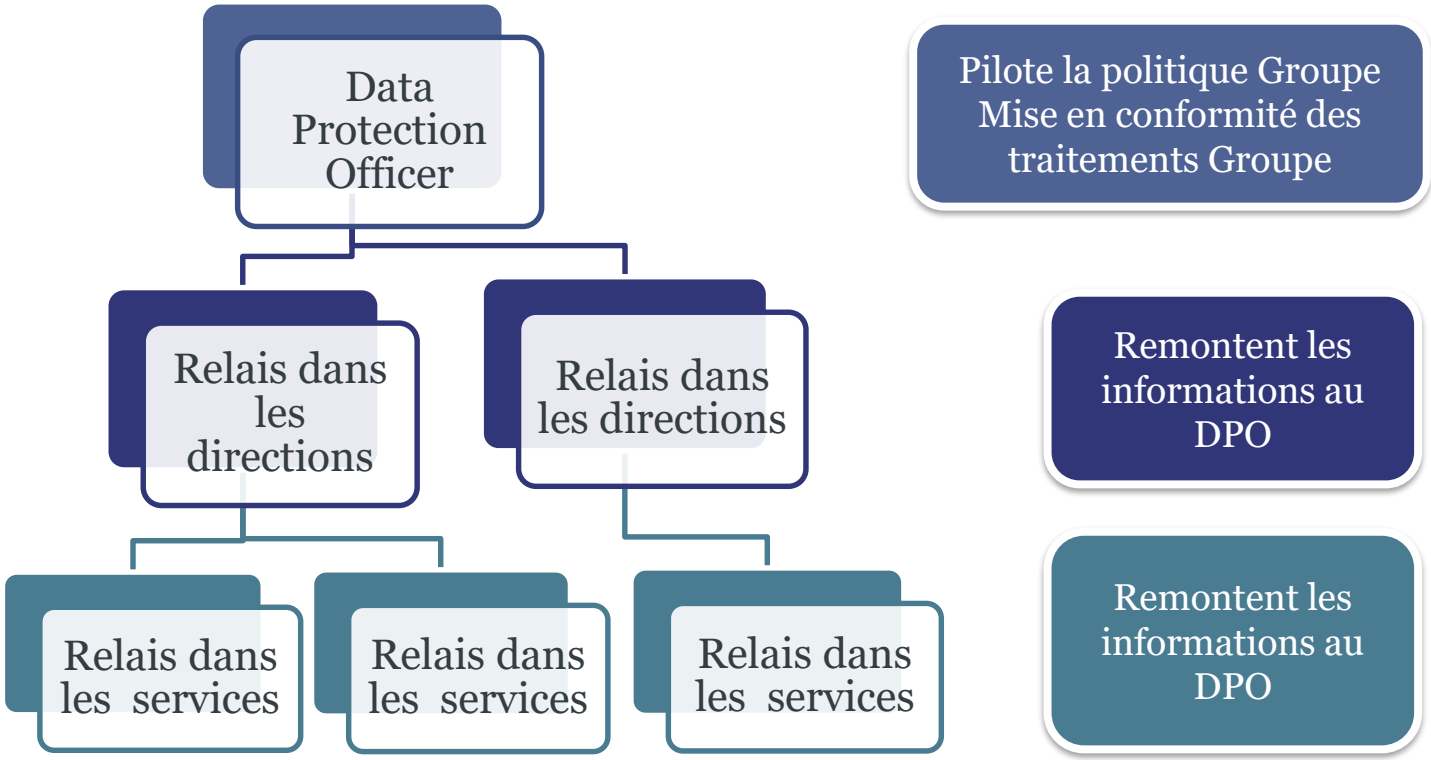
- Responsable de traitement sanctionné : banque en ligne
- Autorité concernée : autorité allemande (Berlin)
- Montant de la sanction: 50 000 €
- Motif :
  - traitement illégal et sans autorisation des données personnelles d'anciens clients d'une banque
    - constitution d'une liste noire d'anciens clients afin de refuser l'ouverture d'un nouveau compte
    - la banque a déclaré être dans l'impossibilité de distinguer les anciens clients "à risque" des anciens clients "non à risque"
    - Absence de base légale pour conserver les données de clients "non à risque" et leur refuser l'ouverture d'un nouveau compte

Bird & Bird

5. Gouvernance DPO

Permettre au DPO d'exercer ses missions

Rôles du DPO: **CONSEILLER** **CONTRÔLER** **PILOTER**



Bird & Bird

6. *Accountability*

Documenter sa conformité

Accountability:

Obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Exemples de documentation d'*accountability*:

- Registre des activités de traitement
- PIA
- *Privacy Policy* - interne à l'entreprise
- *Privacy Policy* - sites internet /applications
- Politique globale de sécurité (*IT Policy*)
- Checklist « *Privacy by design / by default* »
- Politique de conservation des données à caractère personnel
- Mentions d'information des personnes concernées
- Procédure de gestion des violations de données à caractère personnel
- Procédure de gestion des plaintes et d'exercice des droits des personnes concernées

Bird & Bird

7.Formation et sensibilisation des salariés

Diffuser en interne la gouvernance "données personnelles"

- Ateliers de formations thématiques
- Formations par département/ secteur de l'entreprise (RH, marketing, etc.)
- Supports pédagogiques
- Formation e-learning (*la rendre obligatoire lors de l'arrivée d'un salarié ? Optionnelle ?)*
- Formation continue des salariés (*mise à jour des connaissances, suivi de l'actualité juridique et technologique, etc.)*
- Bilan de formation (*besoin d'autres thématiques de formation ? nouvelles formations à envisager ?)*

Bird & Bird

Merci & Bird & Bird

Merav Griguer
Avocat Associée
merav.giguer@twobirds.com

twobirds.com