# Commission nationale pour la protection des données (CNPD)

*Partage d'expériences: Recommandations pratiques après un an de RGPD*

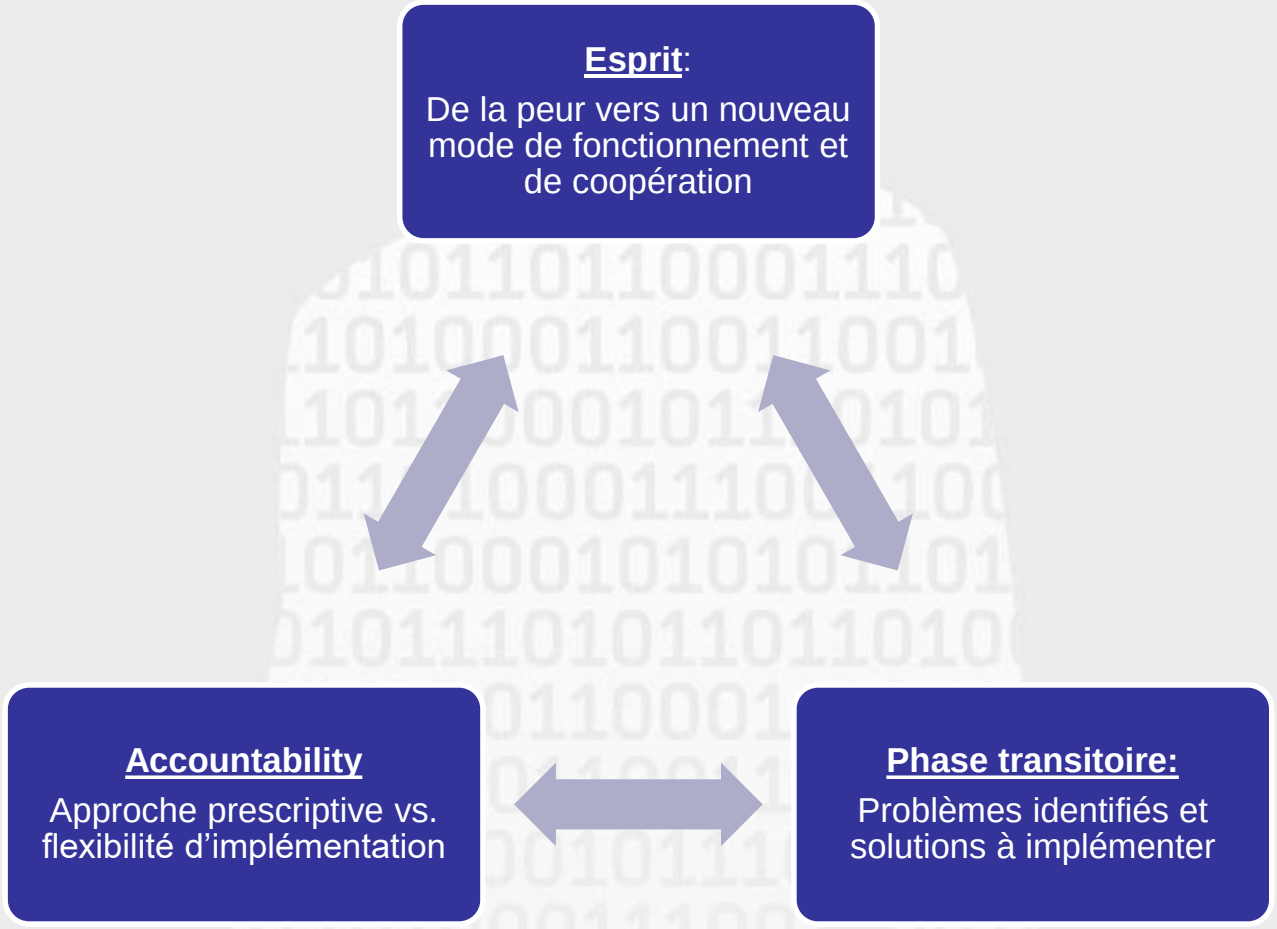

Luxembourg Data Protection Days

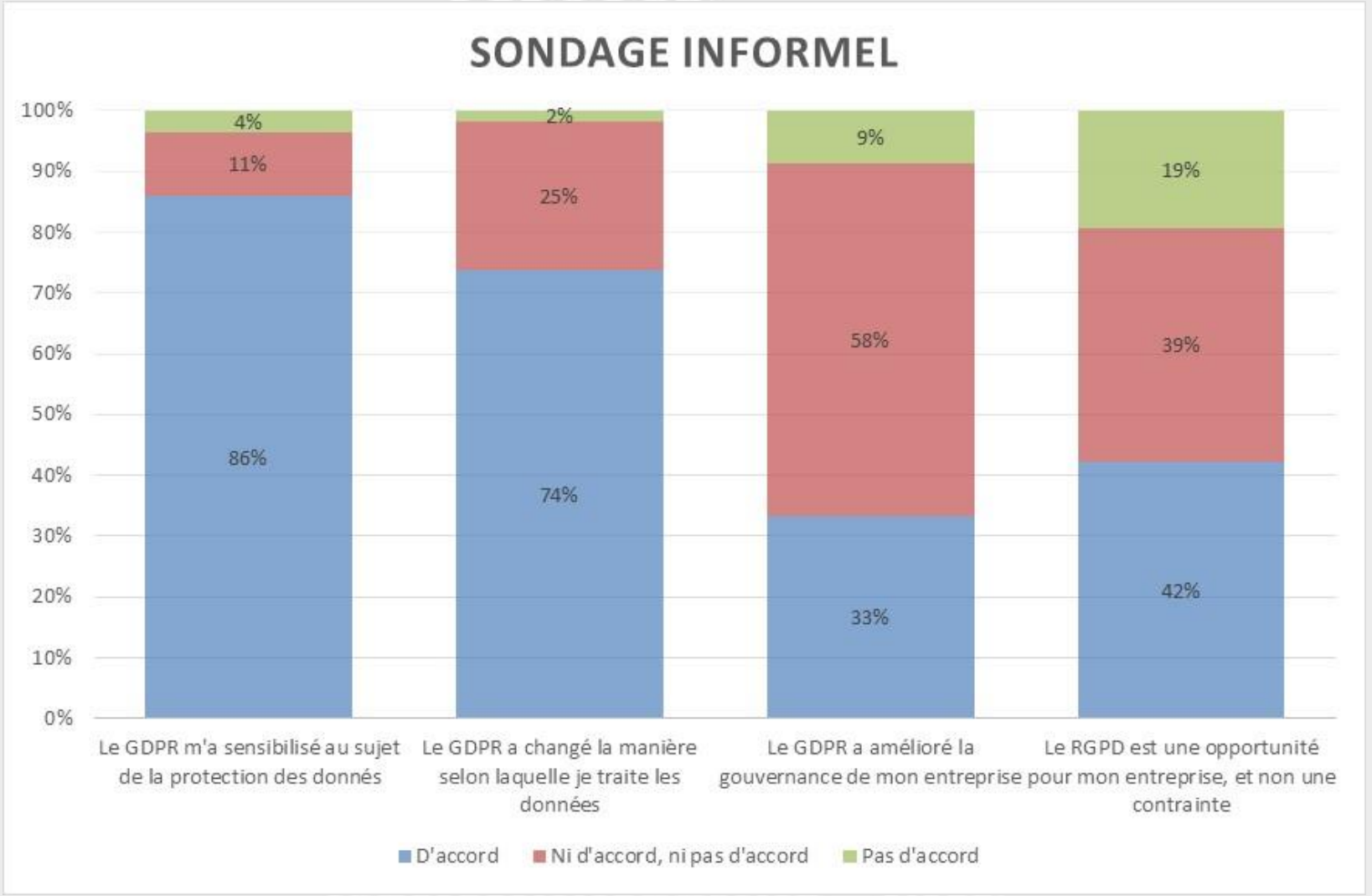
6 – 7 mai 2019

Christophe Buschmann

Commissaire

# Introduction

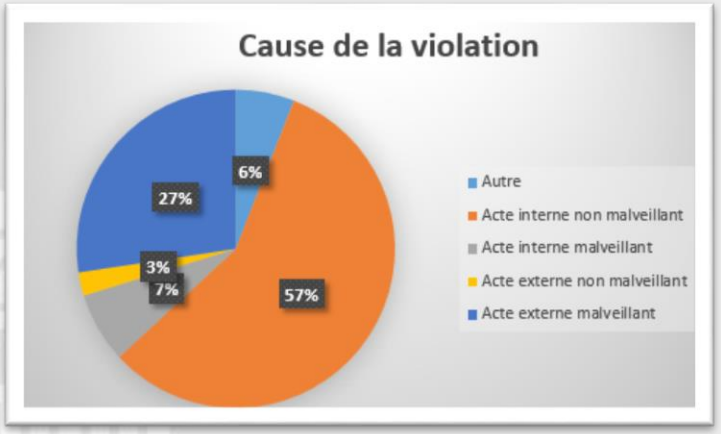



SONDAGE INFORMEL
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
4%
11%
86%
2%
25%
74%
9%
58%
33%
19%
39%
42%
Le GDPR m'a sensibilisé au sujet de la protection des donnés
Le GDPR a changé la manière selon laquelle je traite les données
Le GDPR a amélioré la gouvernance de mon entreprise
Le RGPD est une opportunité pour mon entreprise, et non une contrainte
D'accord
Ni d'accord, ni pas d'accord
Pas d'accord

# Conseils pratiques

## Approche générale

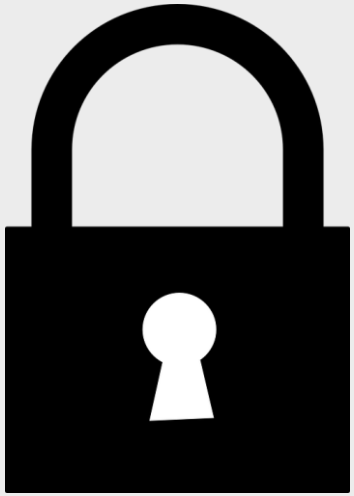
- Fixer les priorités sur base du risque pour les personnes concernées (i.e. pas ce qui est plus/moins difficile, le plus/moins rapide, …)
- Adopter une approche itérative pour implémenter et améliorer le registre (considérer la règle des 80-20)
- Sensibiliser le personnel - la protection des données est avant tout une question de culture d'entreprise et moins un problème purement technique (voir aussi statistiques des violations de données)




# Conseils pratiques

## Communication et sécurité

- Sensibiliser le personnel (57% des violations notifiées sont des actes internes non malveillants – dont plus que la moitié liés à des envois d'emails)
- Mettre en place des mesures de mitigation. Exemples :
  - Encrypter les pièces jointes sensibles
  - Envoyer des liens plutôt que des pièces jointes
  - Utilisation du champs BCC
  - Vérifier la disponibilité de certaines fonctions standard comme (p.ex. une alerte en cas d'envoi externe)
- Identifier les demandeurs avant de répondre en cas d'exercice d'un droit
- Vérifier l'accessibilité de certaines informations



# Conseils pratiques

## Transparence et licéité

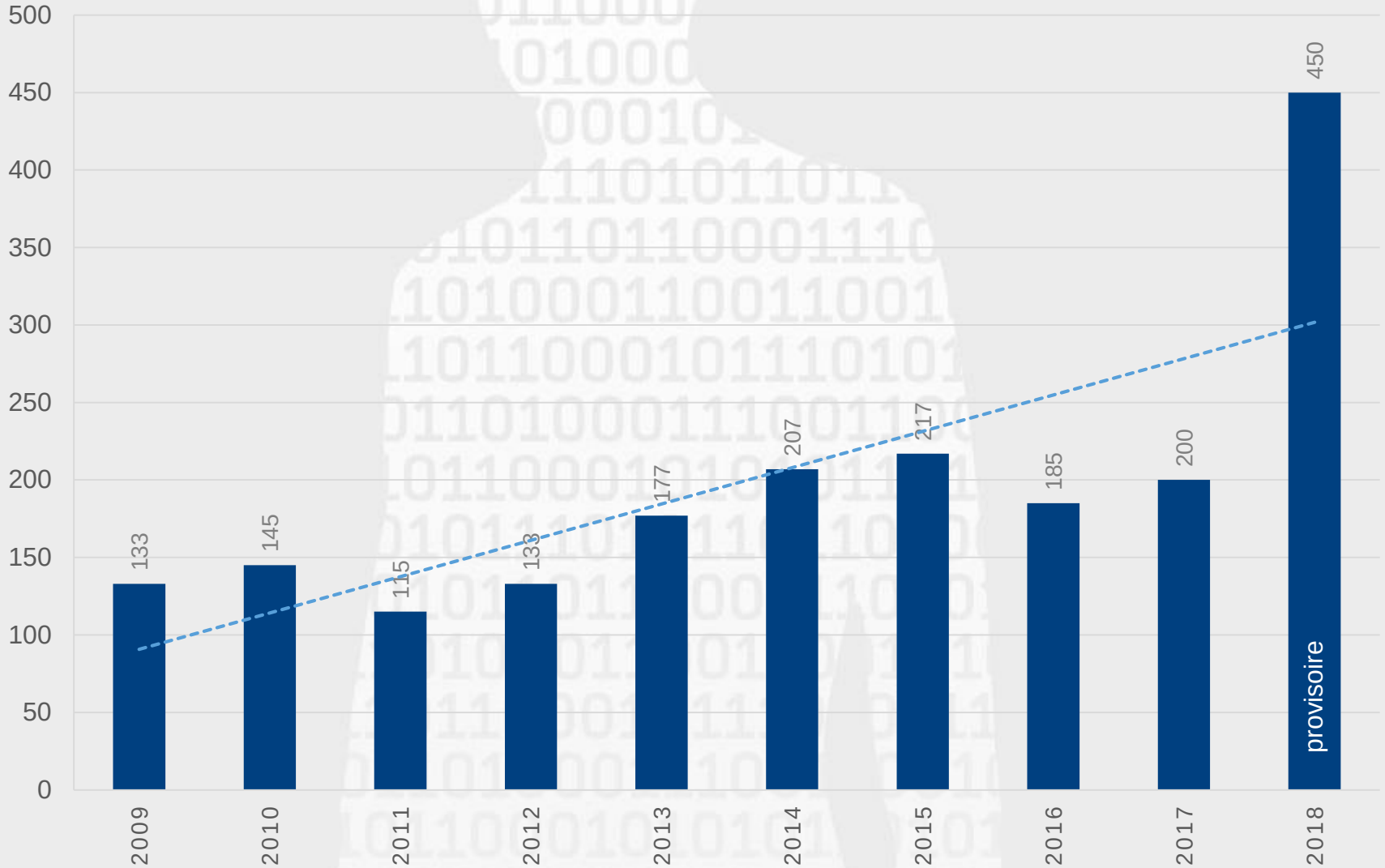
- Ne pas commencer par la conclusion – explorez des alternatives (p.ex. des compteurs au lieux de caméras…)
- Vérifier la granularité et finalité des informations nécessaires (p.ex. religion au lieu des préférences alimentaires)
- Ne pas sur-interpréter le consentement (test à réaliser : qu'est-ce que je peux faire en cas de retrait ?
- Isoler des traitements optionnels avec possibilité d'un consentement (p.ex. pour un archivage à la suite d'un travail presté)
- Mettre l'information là où elle est pertinente (panneaux ou notes au lieu d'une politique difficilement accessible)

# Conseils pratiques

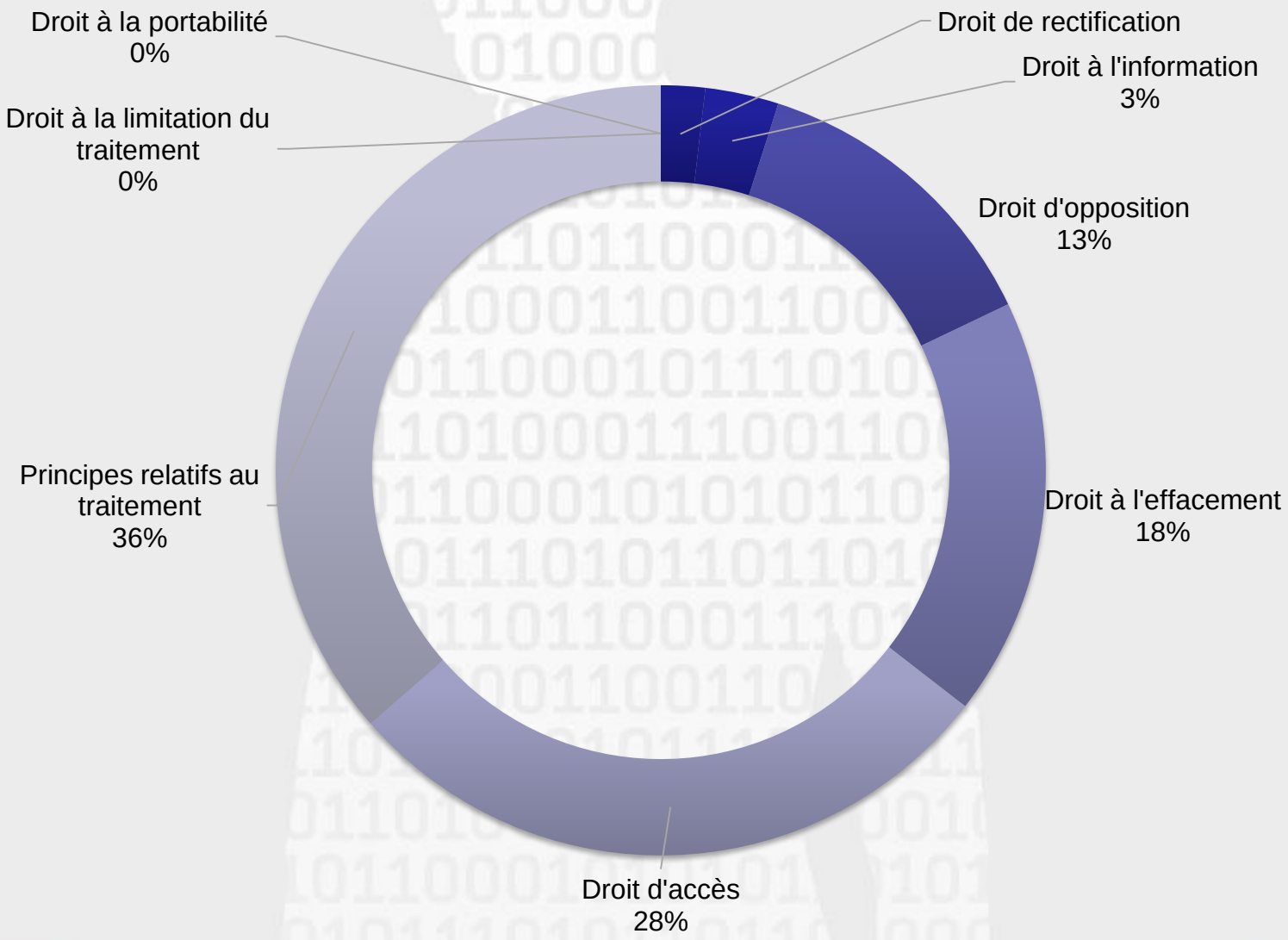
## Accountability

- Parler du bon et du mauvais
- Documenter pour satisfaire un objectif et non pas pour documenter
- Ajuster la documentation à la culture d'entreprise (emails, …)
- Adapter la profondeur de la « due diligence » au risque engagé

# Réclamations



# Réclamations



# Réclamations: Cas pratiques

## Droit d'accès

- Un réclamant s'étonne du montant de sa facture d'électricité et s'interroge sur les index relevés par les compteurs. Il effectue alors une demande d'accès pour obtenir les données qui sont utilisées pour établir la facture et obtenir copie des index pour vérifier s'ils sont corrects selon lui.
  - *Raison : non identification qu'il s'agit d'une demande d'accès.*

- Une société de construction est en litige avec une personne concernée. La personne demande l'accès à ses données personnelles.
  - *Raison : conflit donc refus de faire droit à sa demande alors que les données personnelles doivent lui être communiqués*

## Droit de rectification

- Une banque envoie les extraits de compte par voie postale chez son client. Ce dernier divorce et informe donc sa banque du changement d'adresse. Cette dernière n'effectue pas cette modification en interne. Le plaignant utilise donc son droit à la rectification (art. 16 du RGPD) pour demander de mettre en place son changement d'adresse car il ne souhaite pas que son ex-épouse en prenne connaissance
  - *Raison : il y avait plusieurs bases de données clients. Par conséquent, la modification a été effectuée que partiellement*

# Réclamations: Cas pratiques

## Droit à l'effacement

- Une personne a demandé de fermer son compte mais continue à recevoir la publicité
  - *Raison : effacement de la donnée de manière partielle*

## Licéité d'un traitement

- On me demande de communiquer mon numéro de matricule national pour m'inscrire à une salle de sport (minimisation des données)
  - *Raison : traitement non licite / absence de condition de licéité*

- Mon dossier personnel au sein de mon entreprise est accessible par l'ensemble des salariés de l'entreprise sur un serveur (confidentialité des données).
  - *Raison : manque de mise en place d'une procédure interne*

- Je déclare installer un système de vidéosurveillance à l'accès de mon bâtiment pour veiller à la protection de mes biens mais en réalité je l'utilise pour surveiller les heures d'arrivée et de départ de mes salariés (finalité)
  - *Raison : soupçons que mes salariés ne respectent pas les horaires mais surveillance illicite de base*

# Réclamations: Conseils pratiques

## Recommandations

- Faire un accusé - éviter de laisser les personnes concernées dans le doute
- Assurer de répondre correctement (droit d'opposition est différent du  droit à l'effacement etc …)
- Droit d'accès – ne pas renvoyer à la politique générale mais être précis
- Attention à la sécurité en cas de transfert
- Publier un point de contact clair
- Sensibiliser le personnel pour reconnaitre l'exercice d'un droit

# Recommendations générales

| Je suis parfaitement conforme | Je suis dans une démarche mais probablement pas prêt | Je suis concerné mais pas prêt | Je ne suis pas concerné | Je fais rien et espère ne pas être contrôlé |
|---|---|---|---|---|
| • Partagez vos expériences<br>• Assurez la continuité et l'évolution<br>• Restez attentif<br>• Soyez honnêtes sur ce que vous pouvez assurer | • Adoptez une approche basée sur les risques - Evitez d'être bloqué sur des détails au détriment de points plus importants<br>• Soyez confiants de vos efforts – utilisez un langage adapté aux personnes concernées<br>• Faites bon usage de la guidance désormais disponible au niveau EU<br>• Echangez vous avec d'autres<br>• Soyez spécifique pour votre cas – ne restez pas dans l'abstrait juridique<br>• Laissez vous guider par l'esprit du RGPD (transparence, contrôle, …) et non pas par les sanctions | • Il n'est jamais trop tard pour lancer les démarches – agissez<br>• Restez positifs et constructifs – la peur ou la renonciation sont des mauvais conseillers<br>• Si vous n'étiez déjà pas conforme avec le régime précédent – ayez une approche top down – et ne vous concentrez pas sur les subtils changements – faites un inventaire complet haut niveau que vous déclinez au fur et à mesure | • Assurez vous que c'est vraiment le cas – c'est peu probable – au moins les données de vos salariés sont à gérer<br>• Attention – le RGPD ne se limite pas uniquement aux données dites "sensibles".<br>• Peut être les mesures à mettre en place sont très simples – mais il faudra les mettre en place | • Cette position n'est pas acceptable – les sanctions qui seront prises dans ce cas le reflèteront<br>• Rendez vous compte que vous allez nuire à vos clients, salariés et vous même. Une entreprise qui veut assurer sa pérennité ne peut pas adopter cette approche.<br>• En plus de contrôles "aléatoires" la CNPD effectuera des contrôles ciblés lorsque des violations potentielles sont portées à sa connaissance. Ces éléments peuvent venir de clients, d'(anciens) salariés ou des tiers |

# Partage d'expériences: Recommandations pratiques après un an de RGPD

*Merci pour votre attention!*


Luxembourg
Data Protection Days
6 - 7 Mai 2019

Christophe Buschmann
Commissaire