APDL

Association pour la Protection des Données au Luxembourg

RGPD: PAS À PAS VERS LA CONFORMITÉ

MÉLANIE GAGNON, CIPM, CISA

KEEP CALM AND prepare for GDPR

18 mois pour se conformer

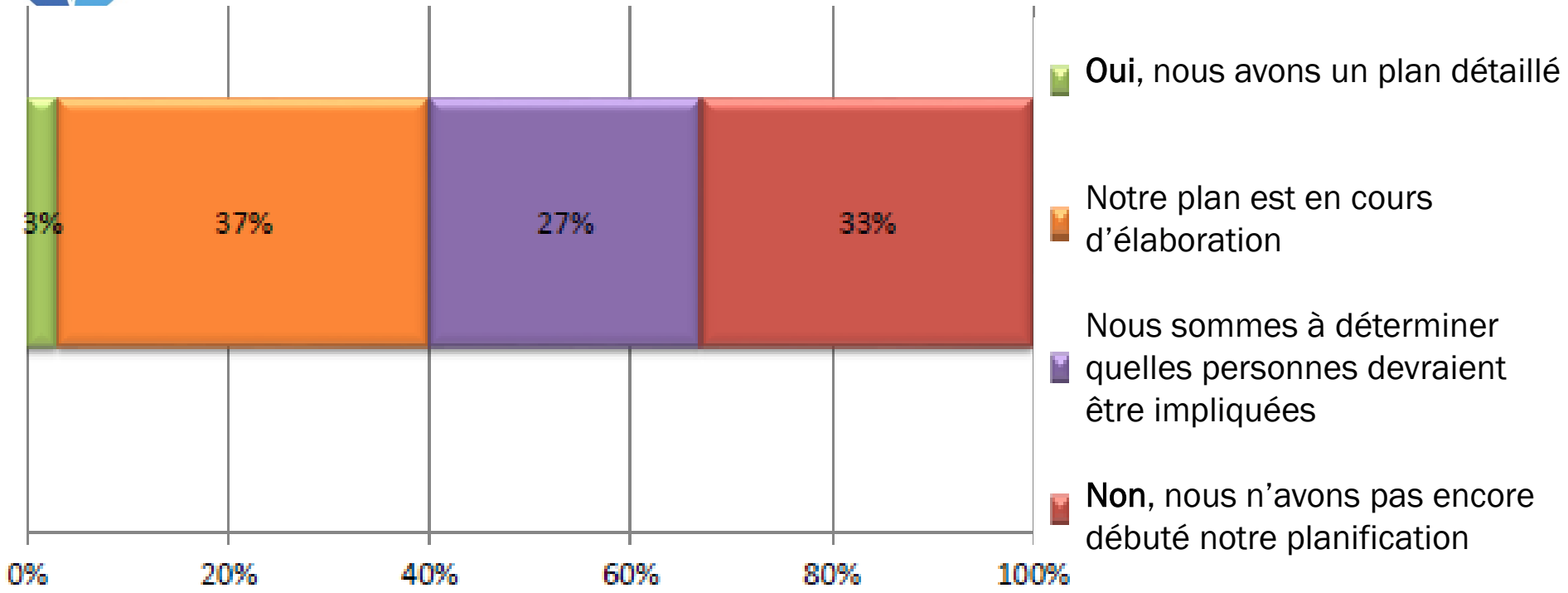
14 Avril 2016

Adoption

25 Mai 2018

Entrée en application

AVEZ-VOUS UN PLAN POUR VOUS PRÉPARER?

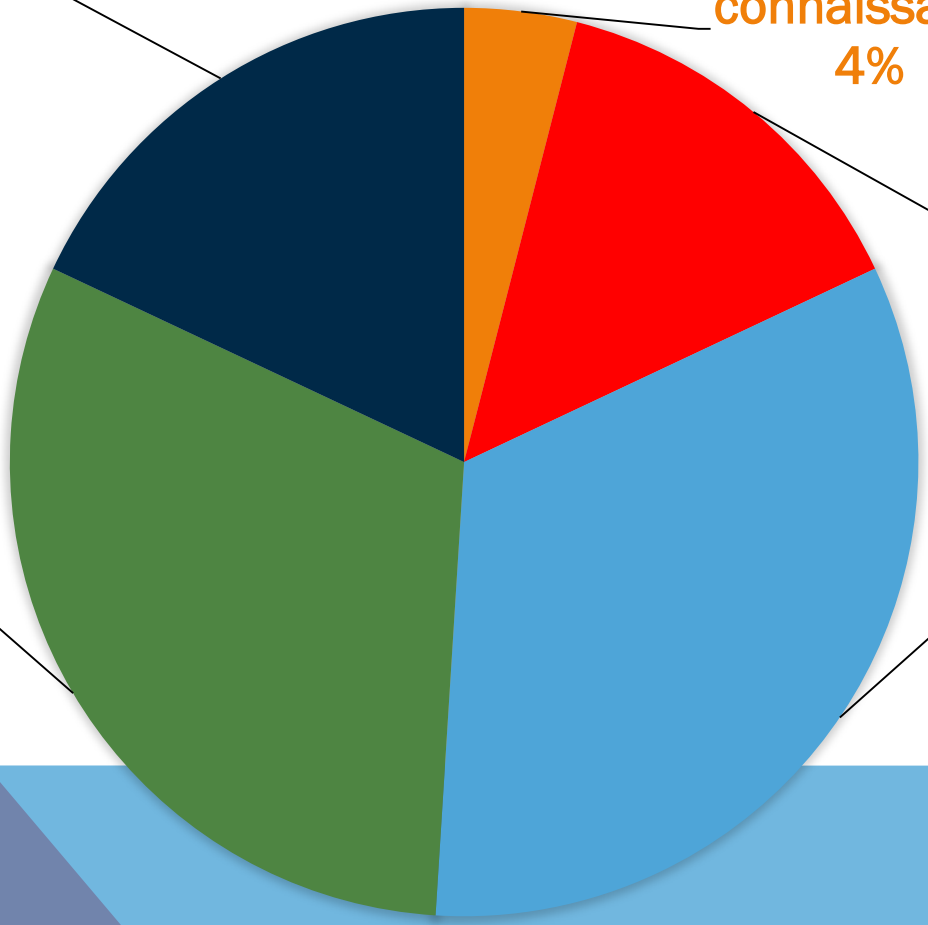


Dimensional research – Sponsored by : DELL
Septembre 2016

Seulement 3% ont un plan détaillé!

Et vous?

COMMENT QUALIFIERIEZ-VOUS VOTRE CONNAISSANCE DU RÈGLEMENT?



Dimensional research -- Sponsored by : DELL
Septembre 2016

SYMANTEC / STATE OF PRIVACY REPORT 2015

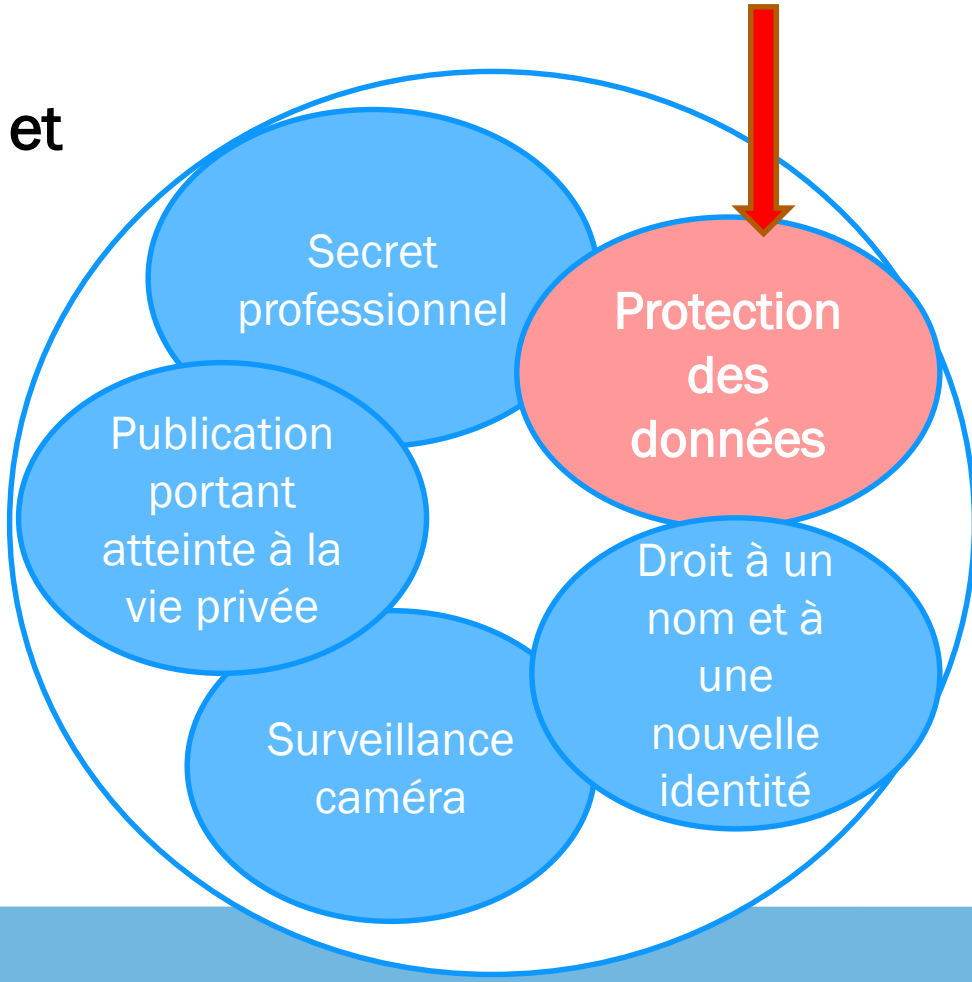
- Définitions
- Préparez-vous en 10 étapes
- Conclusion

VIE PRIVÉE

Droit au respect de sa vie privée et familiale

Ce que:

- Vous faites dans votre vie privée
- Vous faites à votre domicile
- Vous écrivez dans vos courriers ou courriels
- Vous dites au téléphone



PROTECTION DES DONNÉES

Qu'entend-t-on par « protection » des données?

- ✓Droit fondamental
- ✓Protéger les droits et les libertés de la personne concernée
- ✓Concerne les données à caractère personnel

DONNÉE À CARACTÈRE PERSONNEL

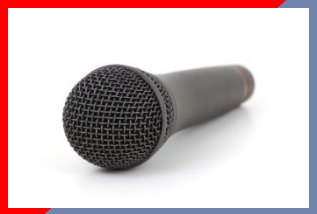
… Toute information se rapportant à une

personne physique identifiée ou identifiable …

… Directement ou indirectement …

Données biométriques, génétiques, concernant

la santé



Réf: Art. 4

DONNÉE À CARACTÈRE PERSONNEL

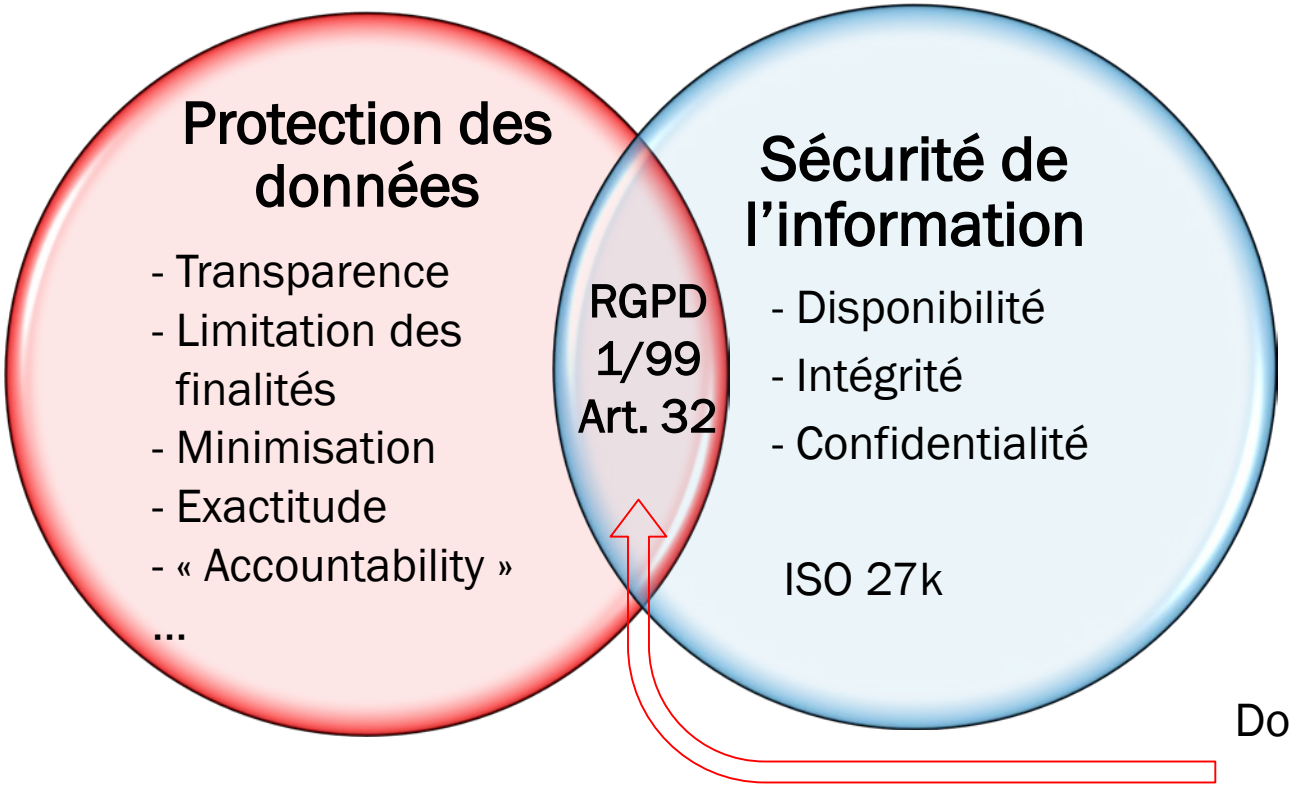
Données collectées lors de l'achat d'un billet d'avion (en ligne)

- Nom, adresse, numéro de téléphone, courriel
- Numéro de passeport / carte d'identité
- Carte de crédit
- Allées et venues (pays visité(s), durée du séjour, autre(s) personne(s), etc.)
- *Adresse IP (dynamique ou non)*

Données cat. particulières

- Allergies
- Maladie
- Besoins particuliers (chaise roulante, handicap, etc.)

PROTECTION DES DONNÉES *ET* SÉCURITÉ



Protection des données ≠ sécurité

SÉCURITÉ DU TRAITEMENT

Article 32

Mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment:

- pseudonymisation et le chiffrement
- confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement
- rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci
- procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures

Tenir compte:

- Coût de mise en œuvre
- Nature, portée, contexte et finalités du traitement
- Risques (degré de probabilité et de gravité varie)

➔ **Risques pour la personne concernée**

Réf: Art. 32

TRAITEMENT DE DONNÉES

… Toute opération ou tout ensemble d'opérations …

… Effectuées ou non à l'aide de procédés automatisés …

…Appliquées à des données ou des ensembles de données à caractère personnel…

Collecte, utilisation, communication, conservation, extraction, rapprochement, diffusion, enregistrement, destruction…

Réf: Art. 4

TRAITEMENT DE DONNÉES

Responsable de traitement

- Personne physique ou morale, autorité publique, le service ou autre organisme
- Détermine les finalités et les moyens du traitement de données à caractère personnel

Sous-traitant

- Personne physique ou morale, autorité publique, le service ou autre organisme
- Traite des données à caractère personnel pour le compte du responsable du traitement

➔ Contrat **écrit** obligatoire entre les 2 parties

Réf: Art. 4

ÊTES-VOUS UN RESPONSABLE DU TRAITEMENT OU UN SOUS-TRAITANT?

Exercice pratique

- Discussion 3 minutes
- Groupe de 2-3 personnes
- Expliquez, pour votre activité principale, si vous êtes un responsable de traitement ou un sous-traitant

Définitions

Préparez-vous en 10 étapes

Conclusion

ÉTAPE 1: PRISE DE CONSCIENCE

Rencontrer	Les personnes clés et les décideurs
Informer	▪ Des changements majeurs à venir ▪ Concepts clés acquis lors de cette séance d'information
Prévoir	▪ Suffisamment de temps! ▪ Un budget suffisant ▪ Ressources suffisantes (internes ou externes) ▪ Une équipe multidisciplinaire pour bâtir le plan de conformité ▪ Formation des employés qui traitent des données à caractère personnel

➔ Il est crucial d'obtenir le **support du management** pour mettre en œuvre un plan de conformité!

ÉTAPE 1: PRISE DE CONSCIENCE

Changements majeurs

- Droits renforcés des personnes concernées – transparence
- Fin des notifications et autorisation (accountability)
- Approche basée sur les risques
- Scope territorial: entreprises hors de l'UE lorsqu'elles offrent des biens ou services sur le marché européen ou surveillent le comportement des résidents européens

Sanctions importantes

- 2% à 4% du chiffre d'affaires annuel mondial de l'entreprise
- 10 ou 20 millions d'euros pour les autres organismes

ÉTAPE 2: REGISTRE DE DONNÉES (INVENTAIRE)

Identifier et documenter tous vos flux de données (clients, employés, etc.)

Quel(s) type(s) de données sont collectées et conservées? Catégorie spéciale?

Quelle est la durée de conservation?

D'où proviennent ces données et qui sont les destinataires?

Où sont stockées les données et qui y a accès?

Quel est le fondement et les finalités des traitements?

Description générale des mesures de sécurité techniques et organisationnelles

Transfert à des tiers ou pays hors UE?

- Obligation de tenir un registre des activités de traitement (RT et S-T)
- Exception : sociétés < 250 employés sauf si le traitement:
  - Comporte un risque pour les droits et libertés
  - S'il n'est pas occasionnel
  - S'il porte sur des cat. particulières ou pénales (art. 9 ou 10)

Réf: Art. 30

ÉTAPE 3: FONDEMENT LÉGAL DU TRAITEMENT

✓ Documentez tous les types de traitement et identifiez le fondement pour chacun:

1. Consentement
2. Exécution d'un contrat
3. Obligation légale
4. Sauvegarde des intérêts vitaux de la personne concernée
5. Intérêt public ou exercice de l'autorité publique
6. Intérêt légitime poursuivis par le responsable de traitement ou un tiers

Le fondement doit être communiqué:

- Dans la déclaration de confidentialité
- Lors d'une demande d'accès par la personne concernée

Réf: Art. 6

ÉTAPE 4: CONSENTEMENT

- ✓ Manifestation active : pas de case cochée préalablement ou absence d'action (opt-in et non opt-out)
- ✓ Consentement explicite pour certains traitements
  - Données sensibles (origine ethnique, opinions politiques, religion, données biométriques, santé, etc…)
  - Profilage
- ✓ Règles spécifiques pour les mineurs (> 13-16)
- ✓ Responsable du traitement a la charge de la preuve
  - Prévoir une piste d'audit pour prouver le consentement
- ✓ La personne concernée a le droit de retirer son consentement à tout moment!

Consentement doit être:

- Libre
- Spécifique
- Éclairé
- Univoque

Réf: Art. 7 et 8

ÉTAPE 5: COMMUNICATION

- ✓Évaluez et révisez votre déclaration de confidentialité existante
- ✓Communication de manière concise, dans une langue compréhensible et claire.

- ✓Nouveaux types d'information à communiquer à la personne concernée:
  - Identité et contact du DPO
  - Fondement légal du traitement de données
  - Délais de conservation
  - Est-ce que les données seront échangées à l'extérieur de l'UE
  - Possibilité pour la personne de porter plainte
  - …

➔ Plus grande transparence envers la personne concernée

Réf: Art. 13

ÉTAPE 6: DROIT DE LA PERSONNE CONCERNÉE

Adaptez vos procédures et prévoyez les ressources suffisantes pour permettre à la personne concernée d'exercer ses (nouveaux) droits renforcés.

- Droit à l'information
- Droit d'accès et de rectification
- **Droit à la limitation du traitement**
- **Droit à l'oubli**
  - Retrait du consentement, traitement illicite, obligation légale, etc.
- **Portabilité des données**
- Objection à l'encontre de prises de décisions automatisées et de **profilage**

➔ Portabilité: guide du WP29 à venir en 2017

Réf: Art. 16 à 22

ÉTAPE 7: VIOLATION DE DONNÉES (1/3)

- Violation de la sécurité
- Accidentel ou illicite
- Provenant de l'interne ou de l'externe

- Destruction
- Perte
- Altération
- Divulgation ou accès non autorisés

➔ Une simple erreur peut mener à une violation de données et avoir des conséquences graves pour les personnes concernées

Réf: Art. 4

ÉTAPE 7: VIOLATION DE DONNÉES (2/3)

Asiana Airlines' customer database leaked

Inquiry launched after HIV clinic reveals hundreds of patients' identities

The 56 Dean Street clinic in London apologises after sending newsletter disclosing names and email addresses of 780 people, many living with HIV

ÉTAPE 7: VIOLATION DE DONNÉES (3/3)

Obligation de notification	
Autorité de contrôle	72 heures
Personnes concernées	Dans les meilleurs délais
Responsable de traitement	Sous-traitant doit notifier dans les meilleurs délais

Exceptions - pas de notification à la personne concernée si:

- N'engendre pas un risque élevé ou le risque est atténué par des mesures de sécurité
- Exigerait des efforts disproportionnés
  - ➔ Dans ce cas: communication publique

Réf: Art. 33 et 34

ÉTAPE 8: PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT ET ANALYSE D'IMPACT

Mesures techniques et organisationnelles appropriées

Dès la conception

- Avant et pendant le traitement
- Respect des principes relatifs aux traitement (ex: minimisation)
- Pseudo-nymisation

Par défaut

- Limiter le traitement aux données nécessaires pour chaque finalité
- Quantité de données collectées et étendue du traitement
- Durée de conservation et accessibilité des données

Pas de collecte de données « au cas où »…

Réf: Art. 25

ÉTAPE 8: PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT ET ANALYSE D'IMPACT

Analyses d'impact préalables si risque élevé, en particulier:

- Évaluation systématique et approfondie d'aspects personnels
- Traitement à grande échelle de catégories particulières de données
- Surveillance systématique à grande échelle d'une zone publique

Consultation préalable de l'autorité de contrôle (CNPD)

- Si le traitement présente un risque élevé, si le responsable de traitement ne prenait pas de mesures pour atténuer le risque

Guide du WP29 à venir en 2017

L'analyse de risques de sécurité de l'information = **impacts sur les données de l'organisation**

L'analyse d'impact sur la protection des données = **impacts sur la personne concernée**

Réf: Art. 35 et 36

ÉTAPE 9: DÉLÉGUÉ À LA PROTECTION DES DONNÉES

DÉSIGNATION OBLIGATOIRE LORSQUE:

- Secteur public
- Suivi régulier et systématique des personnes « à grande échelle »
- Traitement de données « sensibles » ou relatives à des condamnations, également « à grande échelle ».

MISSION

- Informer et conseiller
- Contrôler le respect du règlement
- Sensibilisation et formation
- Conseiller lors des analyses d'impact et en vérifier l'exécution
- Point de contact + coopération avec l'autorité de contrôle

Indépendant

Interne ou externe

Pourquoi attendre le 25 mai 2018 pour nommer un DPO? Il saura vous aider à vous préparer!

Guide du WP29 à venir en 2017

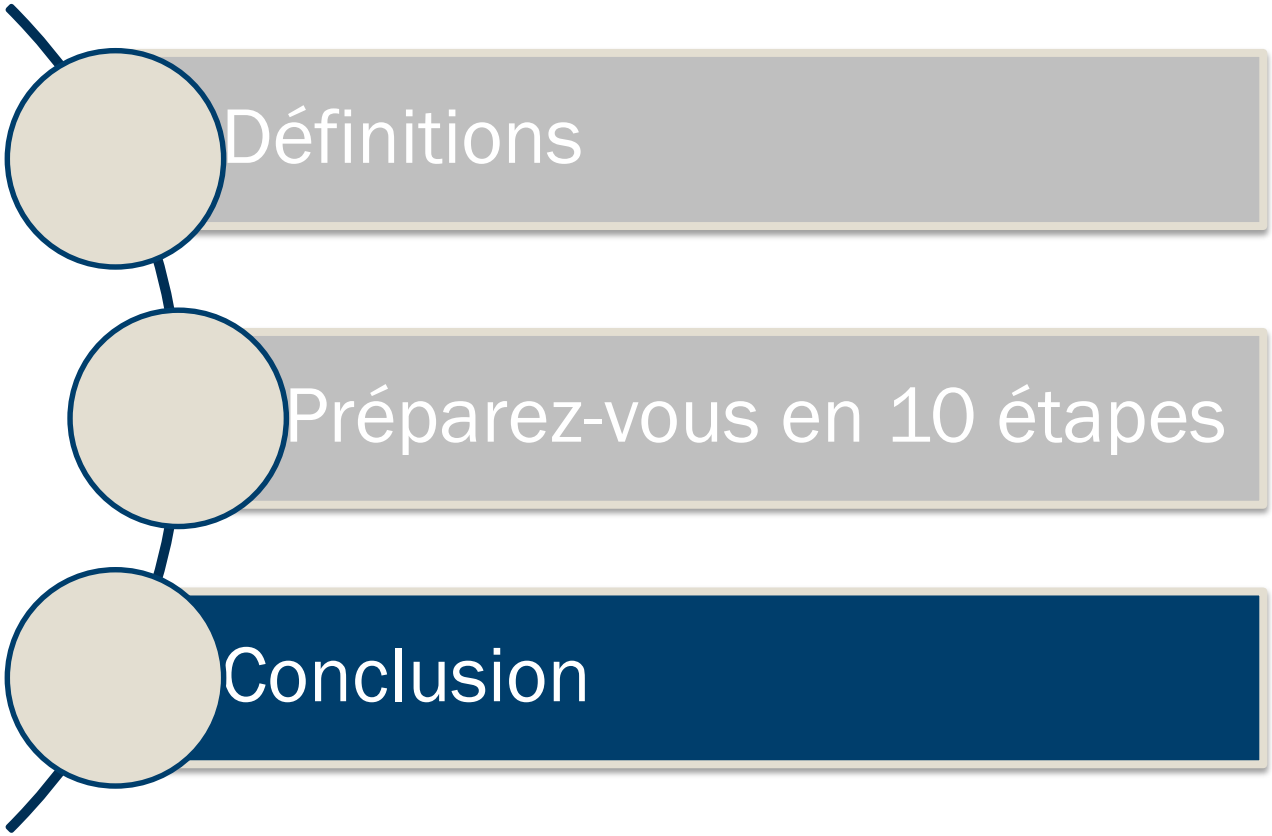
Réf: Art. 37, 38 et 39

ÉTAPE 10: CONTRATS EXISTANTS

Réviser tous les contrats pertinents

- Le traitement par un sous-traitant est régit par un **contrat écrit** ou un **autre acte juridique:**
  - Lie le sous-traitant à l'égard du traitement
  - Définit l'objet et la durée, la nature et la finalité du traitement
  - Le type de données à caractère personnel et les catégories de personnes concernées
  - Obligations et droits du responsable de traitement
- Le responsable de traitement ne fait appel qu'à des sous-traitants qui présentent des garanties suffisantes
- Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable du responsable de traitement

Réf: Art. 28


Définitions
Préparez-vous en 10 étapes
Conclusion

CONCLUSION

Revenons à la 1ère étape: Prise de conscience

Votre mission, si vous l'acceptez…

➔Planifier une rencontre avec vos dirigeants ou votre équipe interne…

…avant le 1er décembre!

Plus que 18 mois pour vous préparer!

MERCI POUR VOTRE ATTENTION

Mélanie Gagnon, CIPM, CISA
www.dataprotection.lu