



Le 7 mars 2018

Présentation RGPD

Règlement Général sur la Protection des Données



Association des
Maires de l'Isère

Programme de la conférence

- **Première Partie**

- Présentation du RGPD au travers des questions fréquemment posées
- Les principes et obligations imposées par le Règlement
- Questions-réponses

- **Deuxième Partie**

- Les solutions pour être en conformité
- Questions-réponses et échanges



Présentation des intervenants (détail en fin de séance)



Présentation du RGPD au travers des questions fréquemment posées

Qu'est-ce que le RGPD ?



L'opinion (09/01/2018)

Présentation du RGPD au travers des questions fréquemment posées

Qu'est-ce que le RGPD ?

Règlement > Directive



Applicabilité : 25 mai 2018

Des principes
Des obligations
Des droits

173 **99**
considérants **articles**

Présentation du RGPD au travers des questions fréquemment posées

Pourquoi un Règlement alors qu'on avait déjà la loi Informatique et Libertés de 1978 ?

- Cadre juridique non respecté
- Cadre juridique non homogène
- Absence de maîtrise des données
- Absence de responsabilité



Présentation du RGPD au travers des questions fréquemment posées

Qu'est-ce qu'une donnée personnelle ?



Présentation du RGPD au travers des questions fréquemment posées

Quelques exemples de traitements de données



- La tenue des registres d'état civil
- l'édition des tables annuelles et décennales
- la transmission des informations à certaines administrations
- la rédaction des actes et l'édition d'extraits et de copies des actes



- La tenue et la gestion de la liste électorale par la commune
- L'utilisation de la liste électorale par le maire
- L'utilisation de la liste électorale par des tiers

Présentation du RGPD au travers des questions fréquemment posées

Quelques exemples de traitements de données



- La fiscalité locale : recueil des **informations fiscales** et communication aux services fiscaux
PS : règles de la diffusion de documents administratifs selon la Loi CADA restent inchangées
- Le fichier des centres communaux d'action sociale (CCAS) contient des informations sur les **conditions de résidence et sur la situation familiale, professionnelle et financière du demandeur**

Présentation du RGPD au travers des questions fréquemment posées

Pourquoi entend-on beaucoup parler du RGPD ?

Renversement

Charge de la preuve

Avant le 25 mai 2018

CNIL.



La CNIL doit prouver la non-conformité des organismes

Après le 25 mai 2018



CNIL.

Les organismes doivent prouver leur conformité à la CNIL

Présentation du RGPD au travers des questions fréquemment posées

Quelle responsabilité pour les élus en cas de non-conformité ?



Présentation du RGPD au travers des questions fréquemment posées

Quelle responsabilité pour les élus en cas de non-conformité ?

Les sanctions

Financières

Amendes administratives
allant jusqu'à

20

millions d'euros d'amende

Pénales

Sanctions pénales allant jusqu'à

5 ans

d'emprisonnement et

300 000 €

d'amende



Présentation du RGPD au travers des questions fréquemment posées

Le RGPD, encore une nouvelle obligation !



PROTECTION

- Protection des données
- Diminution des risques de violation de données
- Confidentialité
- Sécurité



RÉPUTATION

- Respect de la vie privée
- Valeurs exemplaires d'humanisme et de bienveillance



CONFIANCE

- Transparence auprès des citoyens
- Retrouvent une maîtrise des données



Les principes et obligations imposées par le Règlement

Les principes juridiques

Les obligations juridiques

- Principe d'accountability (responsabilisation, transparence)
- Désigner un DPO (délégué à la protection des données)
- Obligations en matière de sous-traitance

Les obligations techniques

- La sécurité physique des données
- La sécurité informatique des données



Les principes et obligations imposées par le Règlement

Le principe de licéité

Quelle est la base juridique du traitement ?

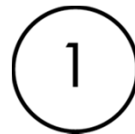


Le principe de conservation limitée des données

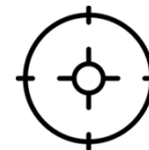


Combien de temps je conserve mes données ?

Le principe de limitation des finalités



Privilégier une finalité par traitement



Le principe d'exactitude des données

Les données sont-elles encore valables ?



Le principe de minimisation des données

Est-ce que toutes les données sont nécessaires ?

Les principes et obligations imposées par le Règlement

Les obligations juridiques

- Principe d'accountability (responsabilisation, transparence)
- Désigner un DPO
- Obligations en matière de sous-traitance



Au revoir les formalités CNIL

Bonjour le registre des traitements



Les principes et obligations imposées par le Règlement

Les obligations juridiques

- Principe d'accountability (responsabilisation, transparence)
- Désigner un DPO
- Obligations en matière de sous-traitance

Gardien des données de l'organisme



Obligatoire pour les services publics



Obligatoire pour certaines entreprises :

- Activité de base reposant sur les données
- Traitement à grande échelle
- Suivi régulier



Profil à dominance juridique



Interne ou externe

Les principes et obligations imposées par le Règlement

Les obligations juridiques

- Principe d'accountability (responsabilisation, transparence)
- Désigner un DPO
- Obligations en matière de sous-traitance

Missions du DPO



Informer et conseiller



Contrôler le respect du RGPD et les sous-traitants



Point de contact avec la CNIL

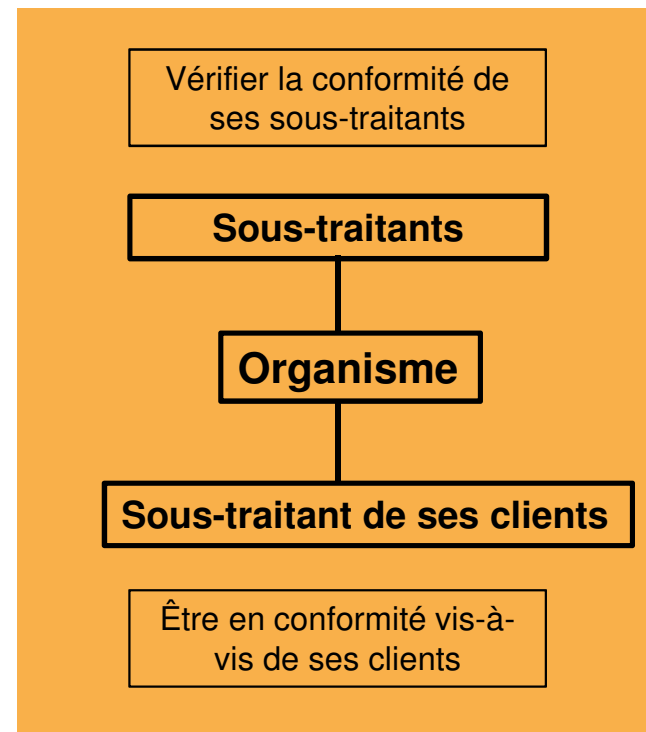


Tenir le registre des traitements

Les principes et obligations imposées par le Règlement

Les obligations juridiques

- Principe d'accountability (responsabilisation, transparence)
- Désigner un DPO
- Obligations en matière de sous-traitance



Les principes et obligations imposées par le Règlement

Les obligations techniques

- La sécurité physique des données
- La sécurité informatique des données



Les principes et obligations imposées par le Règlement

Les obligations techniques

- La sécurité physique des données
- La sécurité informatique des données



Contrôle d'accès des locaux par un badge, fermeture des bureaux à clés, conservation des dossiers dans des armoires fermées à clés, etc.

**Protection des
documents
confidentiels**

Les principes et obligations imposées par le Règlement

Les obligations techniques

- La sécurité physique des données
- La sécurité informatique des données

**17 points de contrôles Minimum
recommandés par la CNIL**



Pour connaître les vulnérabilités de son système d'informations



Échanges et questions-réponses



Les solutions pour être en conformité

- Sensibilisation / formation du personnel
- Désigner un délégué à la protection des données ou un référent
- Audit des traitements de données
- Audit de la sécurité des systèmes d'information



Les solutions pour être en conformité

- Sensibilisation / formation du personnel
- Désigner un délégué à la protection des données ou un référent
- Audit des traitements de données
- Audit de la sécurité des systèmes d'information



- Apprendre les bonnes pratiques
- Comprendre les enjeux de la protection des données
- Éviter les risques de violation de données
- Respecter le Règlement

Les solutions pour être en conformité

- Sensibilisation / formation du personnel
- Désigner un délégué à la protection des données ou un référent
- Audit des traitements de données
- Audit de la sécurité des systèmes d'information



- Créer et tenir un registre des traitements
- Garantir une conformité dans chacun des services et pour l'entreprise
- Établir un point de contact avec la CNIL
- Bénéficier d'un accompagnement juridique et opérationnel

Les solutions pour être en conformité

- Sensibilisation / formation du personnel
- Désigner un délégué à la protection des données ou un référent
- **Audit des traitements de données**
- Audit de la sécurité des systèmes d'information



- Cartographier les traitements de son entreprise
- Évaluer son niveau de conformité
- Définir un plan d'actions correctives prioritaires
- Initier une démarche de conformité au RGPD



Les solutions pour être en conformité

- Sensibilisation / formation du personnel
- Désigner un délégué à la protection des données ou un référent
- **Audit des traitements de données**
- Audit de la sécurité des systèmes d'information

NOM DU TRAITEMENT	GESTION ADMINISTRATIVE DU PERSONNEL
Nom et coordonnées du RT	
Nom et coordonnées du DPO	
Finalité(s) du traitement	
Catégorie(s) de personne(s) concernée(s)	
Catégorie(s) de DCP	
Catégorie(s) de destinataire(s)	
Délai d'effacement	
Mesures de sécurité techniques et organisationnelles	
Transfert de données vers pays tiers / OI	

Les solutions pour être en conformité

- Sensibilisation / formation du personnel
 - Désigner un délégué à la protection des données ou un référent
 - Audit des traitements de données
 - **Audit de la sécurité des systèmes d'information**
- 
- Connaître les vulnérabilités des systèmes d'informations
 - Bénéficier de recommandations en matières de sécurité informatique
 - Avoir un plan d'actions correctives pour sécuriser les systèmes d'information

Les solutions pour être en conformité

1. Sensibiliser les utilisateurs
2. Authentifier les utilisateurs
3. Gérer les habilitations
4. Tracer les accès et gérer les incidents
5. Sécuriser les postes de travail
6. Sécuriser l'informatique mobile
7. Protéger le réseau informatique interne
8. Sécuriser les serveurs
9. Sécuriser les sites web

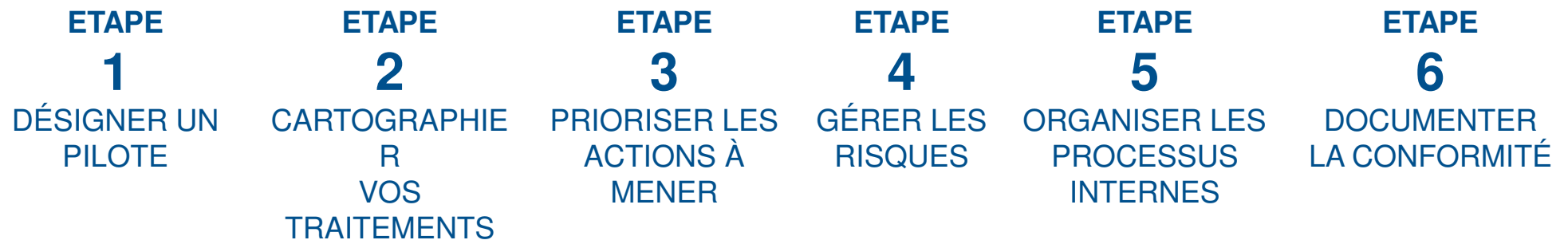


10. Sauvegarder et prévoir la continuité d'activité
11. Archiver de manière sécurisée
12. Encadrer la maintenance et la destruction des données
13. Gérer la sous-traitance
14. Sécuriser les échanges avec d'autres organismes
15. Protéger les locaux
16. Encadrer les développements informatiques
17. Utiliser des fonctions cryptographiques

Conclusion

Comment initier une démarche au RGPD ?

Se préparer en 6 étapes (recommandations CNIL)



Conclusion

Que faire concrètement ?

**DÉSIGNER UN DPO
INTERNE OU EXTERNE**

Mutualisé ou non

**METTRE À JOUR
LA DOCUMENTATION
D'APPEL D'OFFRES
DES MARCHÉS PUBLICS**

Afin d'obtenir des partenaires et sous-traitants des garanties sérieuses, mais aussi de limiter sa responsabilité

**FAIRE UN AUDIT
DE SES TRAITEMENTS**

**FAIRE UN AUDIT
DE SECURITE
INFORMATIQUE**

**ADAPTER
LES MENTIONS LÉGALES,
LES FORMULAIRES,
LES SITES INTERNET,
LES CGV/CGU**

Pour garantir l'information des administrés

**SENSIBILISER ET
FORMER LES AGENTS**

Ateliers de formation, fiches pratiques, etc.

**CRÉER ET/OU
METTRE À JOUR
LA DOCUMENTATION ET
LES PROCÉDURES
INTERNES**

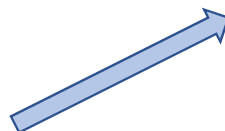
Registre des traitements, procédure en cas de violation de données

Possibilité d'accompagnement/formation spécifique pour une collectivité – AMI/Covateam & Optimex data

**AUDIT
RGPD**



**AUDIT
SÉCURITÉ**



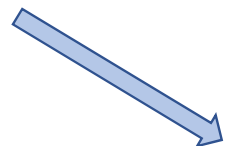
FORMATION DPO

(SI DPO INTERNE)
= FORMATION AU MÉTIER DE DPO
POUR LA PERSONNE RÉFÉRENTE EN



ACCOMPAGNEMENT DPO

Accompagnement du DPO interne
dans la mise en place de ses missions



FORMATION RGPD

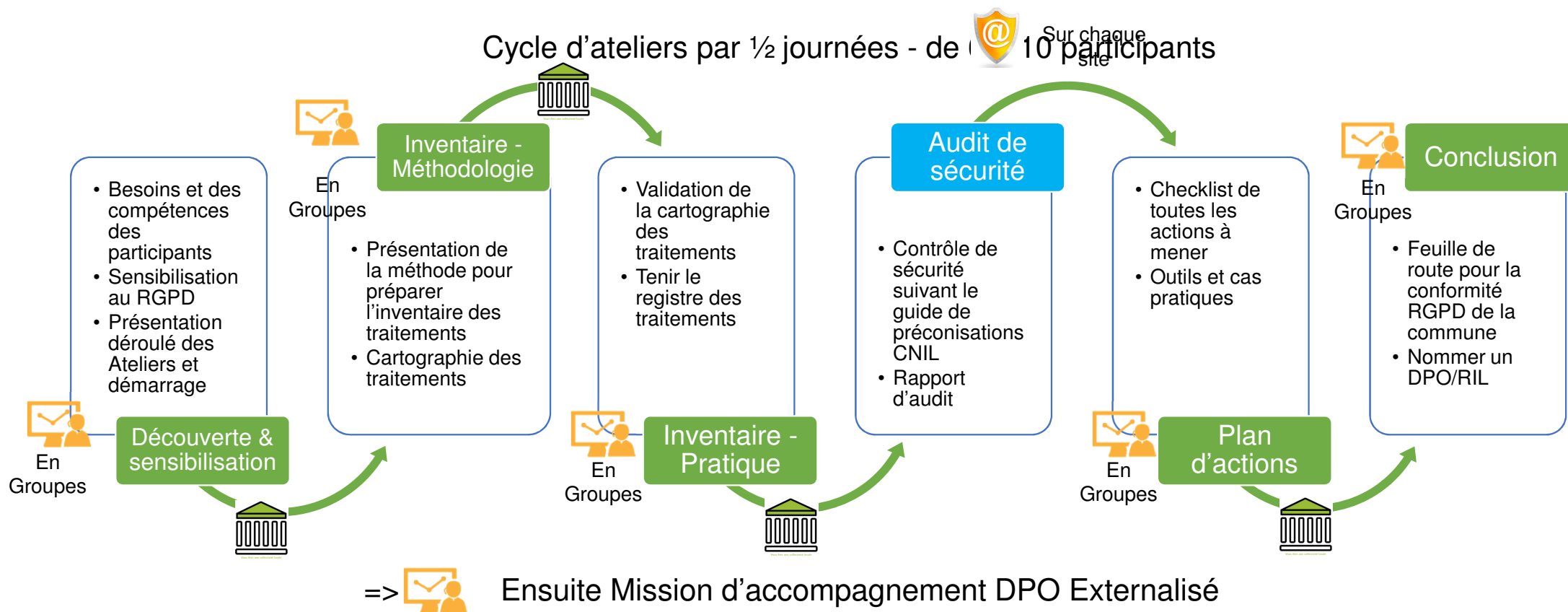
(SI DPO EXTERNE)
= Formation au règlement européen
pour le relais en interne



DPO EXTERNALISÉ

Possibilité d'accompagnement/formation mutualisé sur plusieurs collectivités

AMI/Covateam & Optimex data



Échanges et questions-réponses



Présentation de Covateam

Accompagnement des Entreprises et Collectivités dans la mise en œuvre d'usages et d'outils informatiques performants.

Des experts en temps partagé

INFORMATIQUE – DIGITAL – SECURITE INFORMATIQUE



20 ans d'expérience
services informatiques
usages numériques

5
Consultants



600 jrs de missions
en 2017

Présentation d'Optimex Data

Entreprises, Secteur Public et Associations font appel à nos services pour **externaliser** la gestion de leur projet RGPD

FORMATION



AUDIT



MISSION DPO



L'équipe

Juristes en protection des données

CNIL

AFCDP
Association Française
des Correspondants à la protection
des Données à caractère Personnel

Merci pour votre attention



Tél. : 04 58 00 30 33

E-mail :

philippe.dujardin@covateam.com

Site Internet : www.covateam.com



Tél. : 09 71 16 15 42

E-mail : contact@optimex-data.fr

Site Internet : www.optimex-data.fr

