RGPD

Préparez votre entreprise

LE 25 AVRIL 2019

cci NOUVELLE-CALÉDONIE

Moehau Huioutu

Chargée d'études juridiques à la Cellule économ

L'APPLICATION EN NOUVELLE-CALÉDONIE DE LA RÈGLEMENTATION INFORMATIQUE ET LIBERTÉS

econum
ÉCONOMIE NUMÉRIQUE DE LA NOUVELLE-CALÉDONIE

GOUVERNEMENT DE LA NOUVELLE-CALÉDONIE

Clé n°1 : RGPD

- **Règlement sur la protection des données personnelles**
  - Réforme de la règlementation Informatique et Libertés dans l'Union européenne
- But :
  - **Mieux protéger les données personnelles** face aux GAFAM
- Entré en vigueur dans l'UE :
  - 25 mai 2018

CLÉ N°2 : LA NC -> PTOM

- La NC n'est pas un Etat membre de l'UE…
- … mais un **PTOM**

- La conséquence :
  - La règlementation de l'UE n'est pas directement applicable localement

CLÉ N°3 : PROTECTION DES DONNÉES PERSONNELLES COMPÉTENCE DE L'ÉTAT

- **Compétence de l'Etat :**
  - Répartition des compétences prévue par la loi organique du 19 mars 1999 relative à la NC
- But de la loi informatique et libertés : **protéger la vie privée**
  - Domaine de la **garantie des libertés publiques**

CLÉ N°4 : CADRE APPLICABLE AUJOURD'HUI EN NC

- **Textes de référence** :
  - Loi informatique et libertés du 6 janvier 1978
  - Décret d'application du 20 octobre de 2005
- **Autorité de référence** :

CNIL
Commission Nationale de l'Informatique et des Libertés

- **Présidente :** Marie-Laure Denis

CLÉ N°5 : EVOLUTION DE LA RÈGLEMENTATION EN MÉTROPOLE

- **Loi du 20 juin 2018**
  - Prise en compte des impacts du RGPD
  - Modification de la loi I&L
- **Pas applicable en NC**

CLÉ N°5 : EVOLUTION DE LA RÈGLEMENTATION EN MÉTROPOLE

- **Ordonnance du 12 décembre 2018**
- Art. 1er : **réécrit totalement la loi I&L**
  - Objectif : Meilleure compréhension
  - **Future version loi I&L**
- Art. 29 : **entrée en vigueur**
  - **En même temps que le décret d'application et au plus tard le 1er juin 2019**

CLÉ N°6 : APPLICATION EN NC DE LA FUTURE VERSION LOI I&L

- **Application en NC** (Art. 125) :
  - la loi I&L est applicable en NC dans sa rédaction résultant de l'ordonnance du 12 décembre 2018
- Art. 126 : La référence au RGPD est remplacée par la référence aux règles en vigueur en métropole en vertu du RGPD
  - Seules les dispositions du RGPD dont il est fait référence dans la loi I&L sont applicables en NC ?
  - Le RGPD n'est pas en soi applicable en NC, car NC est un PTOM (Art. 126)
- Aujourd'hui, il faut donc combiner loi I&L et les articles RGPD applicables pour avoir le cadre juridique complet

POUR RÉSUMER…

- Application de la nouvelle réforme informatique et libertés en NC
- Au plus tard le **1er juin 2019** :
  - Ou avec la publication du décret d'application de la loi I&L

CABINET D'AVOCATS FRANCK ROYANEZ

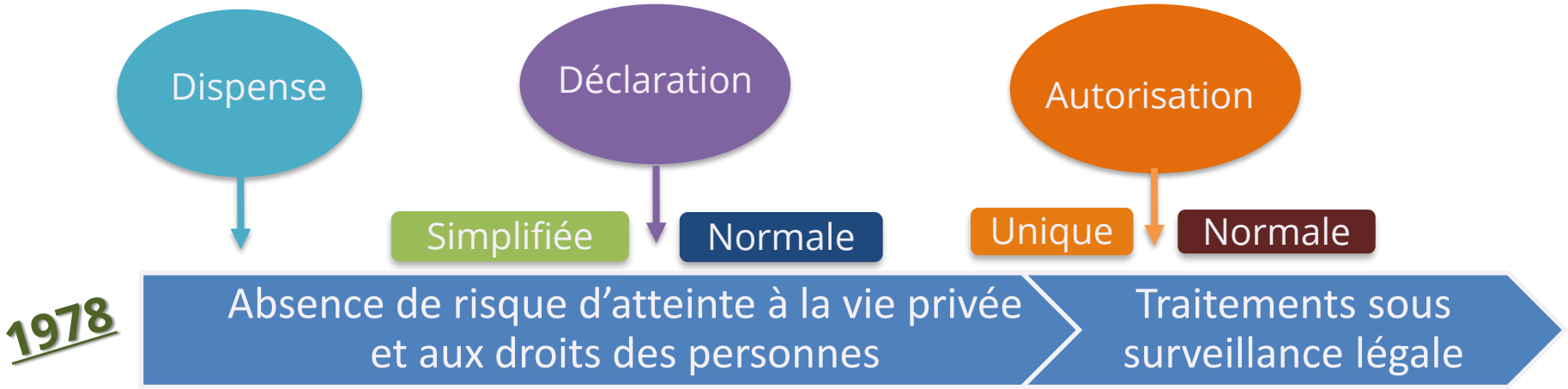
Franck Royanez

Avocat à la Cour

Ancien Bâtonnier

cci NOUVELLE-CALÉDONIE

Le RGPD : de la disparition des formalités à la responsabilité



RGPD

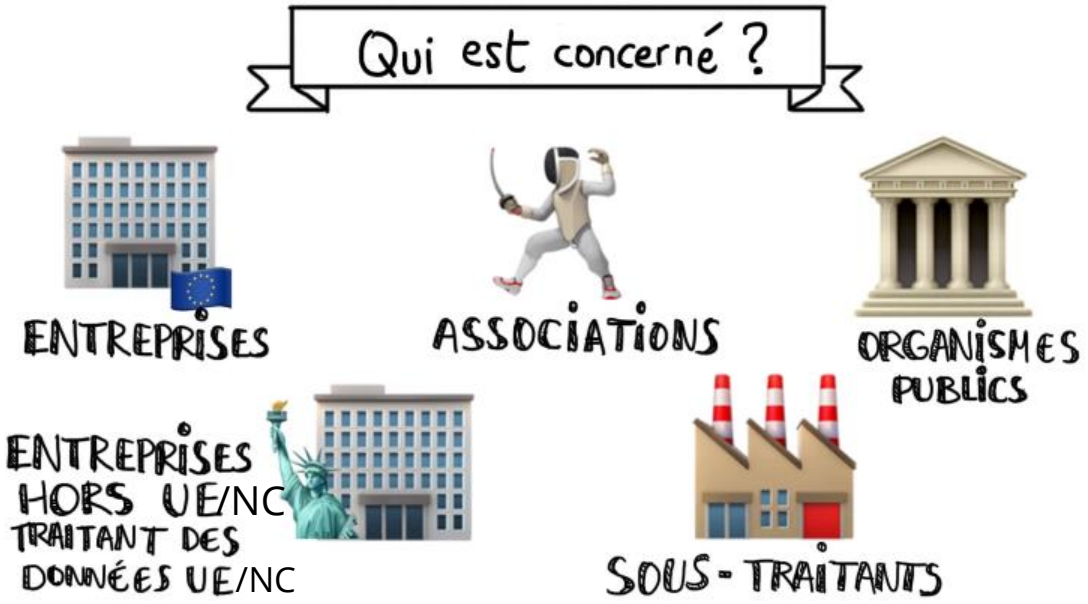
Principe général : la responsabilisation

Avec le RGPD, le traitement doit être en conformité avec ses dispositions et le responsable doit être en mesure de démontrer cette conformité.

Qui est concerné ?

1) Toutes les entités

Privés ou publics, quelle que soit leur taille, devront se mettre en conformité au règlement à partir du moment où leur activité touche aux données personnelles : PME, EPIC, collectivités…



2) Toutes les activités

Et non pas uniquement celles qui ont pour finalité l'utilisation, le stockage ou la collecte de données personnelles.

Qui est concerné ?

3) Les acteurs de l'entreprise

Le responsable du traitement (RDT)

- Détermine la finalité du traitement
- Chef d'entreprise, directeur, un délégué
- Seul responsable de la conformité au RGPD

Les services opérationnels

- RH
- DSI
- COMMERCIAUX
- MARKETING…

Le délégué à la protection

- Interne ou externe
- Mission d'information, de conseil et de contrôle

Le sous-traitant

Même si ce n'est pas sa mission première, il traite des données personnelles pour le compte du RDT.

Les étapes

Ce délégué peut être désigné en interne ou en externe.
Il maîtrise parfaitement les législations sur la protection des données et le RGPD

ETAPE 1
DESIGNER UN PILOTE

Le pilote est un Data Protection Officer

❑ Pour tous les **organismes publics**

❑ Pour les entreprises :

✓ Qui traitent des **données sensibles** (biométriques, religieuses…) ou relatives à des condamnations pénales et infractions

✓ Ou dont **l'activité de base** consiste en un **suivi régulier et systématique des personnes à grande échelle** *

La législation exige du DPO **des compétences** juridiques et techniques, et renforce son indépendance (c'est un **auditeur** interne).

Les étapes

ETAPE 2
CARTOGRAPHIER

1) **Lister** l'ensemble des traitements de données personnelles, informatisées ou non (archives papier) et créer un **registre**. *

2) **Identifier** :

✓ Les processus concernés par le RGPD *

✓ Les risques pour les droits des personnes. *
Il existe neuf critères pour mesurer ce risque.

Pour dresser cette cartographie, les métiers sont mis à contribution, notamment le marketing et la DRH qui gèrent un grand nombre de données nominatives.

Les étapes

Sur la base du registre : 1) Identifier les actions à mener pour être conforme.

2) Les prioriser au regard des risques de ces traitements sur les droits et les libertés des personnes.

ETAPE 3
PRIORISER

Identifier la base juridique fondant le traitement (par ex. consentement de la personne, intérêt légitime, contrat, obligation légale).

Vérifiez que vos **sous-traitants** connaissent leurs nouvelles obligations et l'existence des clauses dans les contrats de S.T.

Vérifiez les **mesures de sécurité** mises en place.

Limiter le traitement aux seules données nécessaires à la poursuite des objectifs.

Révisez vos **mentions d'information** afin qu'elles soient conformes aux exigences du règlement.

Prévoyez les modalités d'exercice des **droits des personnes** concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...).

Les étapes

Si des risques élevés pour les droits et libertés des personnes : **analyse d'impact pour la protection des données** (AIPD).

ETAPE 4
GÉRER LES RISQUES

Il faut faire une AIPD, si au moins **deux** des critères de risques précédemment exposés sont remplis

L'AIPD réalisée par le RDT et le DPO :

- ❑ **Décrit le traitement** concerné et ses finalités.
- ❑ **Evalue la nécessité de son maintien** et sa proportionnalité par rapport aux finalités.
- ❑ **Evalue les risques** pour les droits des personnes.
- ❑ **Démontre la conformité** du traitement au RGPD et en particulier le respect total des droits fondamentaux et les mesures techniques et d'organisation de gestion des risques sur la vie privée.

Les étapes

Le but : **garantir la protection des données à tout moment**, quels que soient les événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire, etc.).

ETAPE 5
ORGANISER

Concrètement, **l'entreprise** :

- **Met en place la protection dès la conception** d'un traitement : minimisation de la collecte de données, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données.
- **Organise la remontée d'information** : formation, responsabilisation des acteurs impliqués et communication interne.
- **Traite les réclamations** (droits d'accès, de rectification, d'opposition, portabilité, retrait du consentement en définissant les acteurs et les modalités.
- **Anticipe les risques de violations de données** et le cas échéant les modalités de la notification à la CNIL et aux personnes concernées.

Les étapes

Documenter la conformité

Prouver votre conformité : constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

ETAPE 6
DOCUMENTER

Information des tiers

- Les **mentions d'information**
- Les modèles de **recueil du consentement** des personnes concernées
- Les procédures mises en place pour l'exercice des droits.

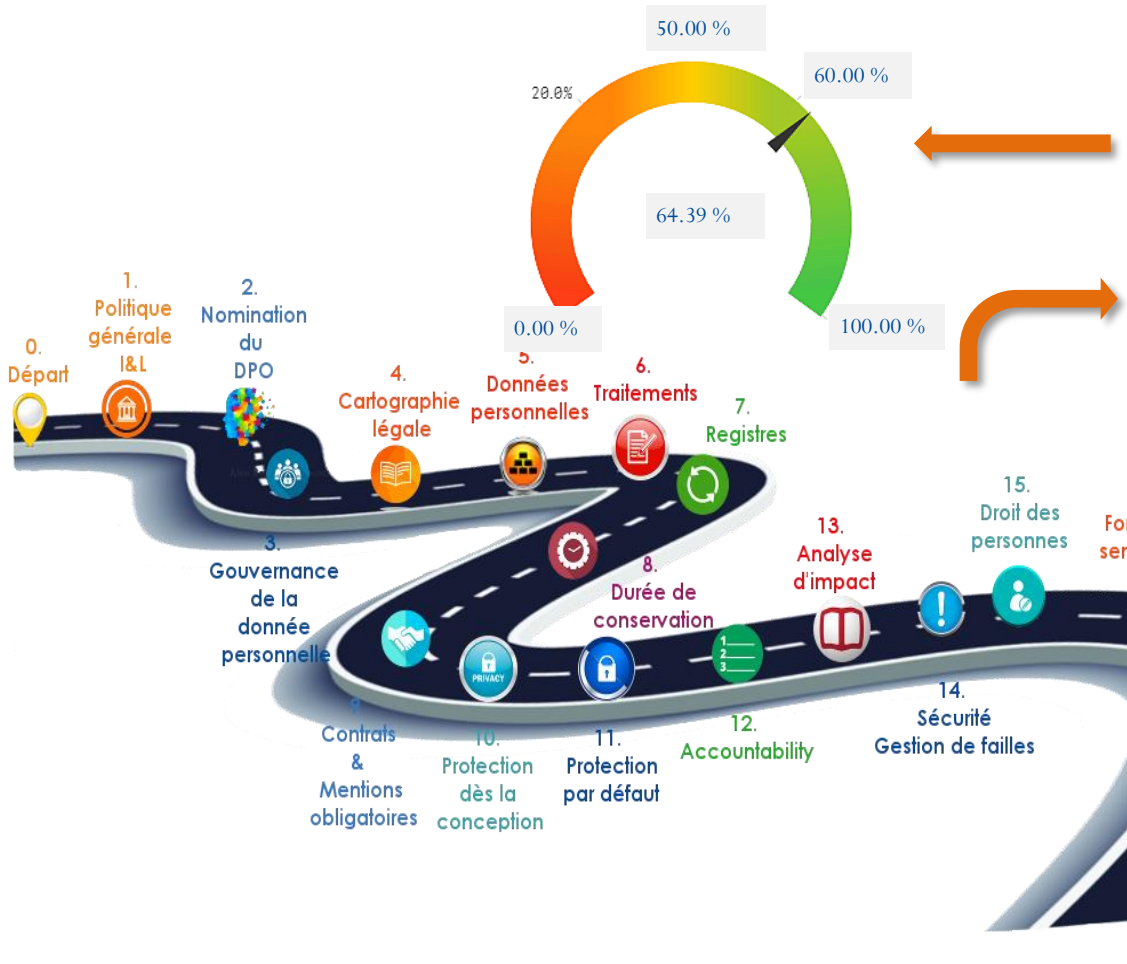
Les contrats

- Les contrats avec les **sous-traitants**
- Les **clauses générales** entre professionnels
- Les clauses avec les clients.

Documentation interne

- **Le registre des traitements**
- **Les AIPD**
- **Les documents encadrant les transferts** de données hors NC & UE (certifications, clauses contractuelles types…)
- La **procédure à suivre en cas de faille**.

Points de contrôle



N°	ETAPE	TITRE	COMMENTAIRE
1.	0	Départ	Ensemble des documents permettant l'initialisation de la norme tels que : - les extraits Kbis ; - l'organigramme de la société ; - la liste des projets ; - etc.
2.	1	Politique générale Informatique et libertés	La politique consiste à mettre l'entreprise en position de conformité à la réglementation de la protection des données. Elle comprend notamment : - la lettre d'information de la Direction générale de l'entreprise ; - la politique interne (collaborateur) et externe (tiers) d'organisation de la protection des données ; - la charte informatique et libertés - etc.
3.	2	Nomination du DPO	Cette étape porte sur l'ensemble du processus de désignation du DPO. Elle comprend notamment : - la lettre de nomination du DPO - la publication des coordonnées du DPO - la lettre d'acceptation de la mission du DPO ; - la lettre d'information à la Cnil ; - la notice d'information des salariés ; - etc.

Les étapes

ÉTAPE 1
DÉSIGNER UN PILOTE

ÉTAPE 2
CARTOGRAPHIER

ÉTAPE 3
PRIORISER

ÉTAPE 4
GÉRER LES RISQUES

ÉTAPE 5
ORGANISER

ÉTAPE 6
DOCUMENTER

QUESTIONS

OPEN
Nouvelle-caledonie
Organisation des Professionnels de l'Economie Numérique

Hatem Bellagi

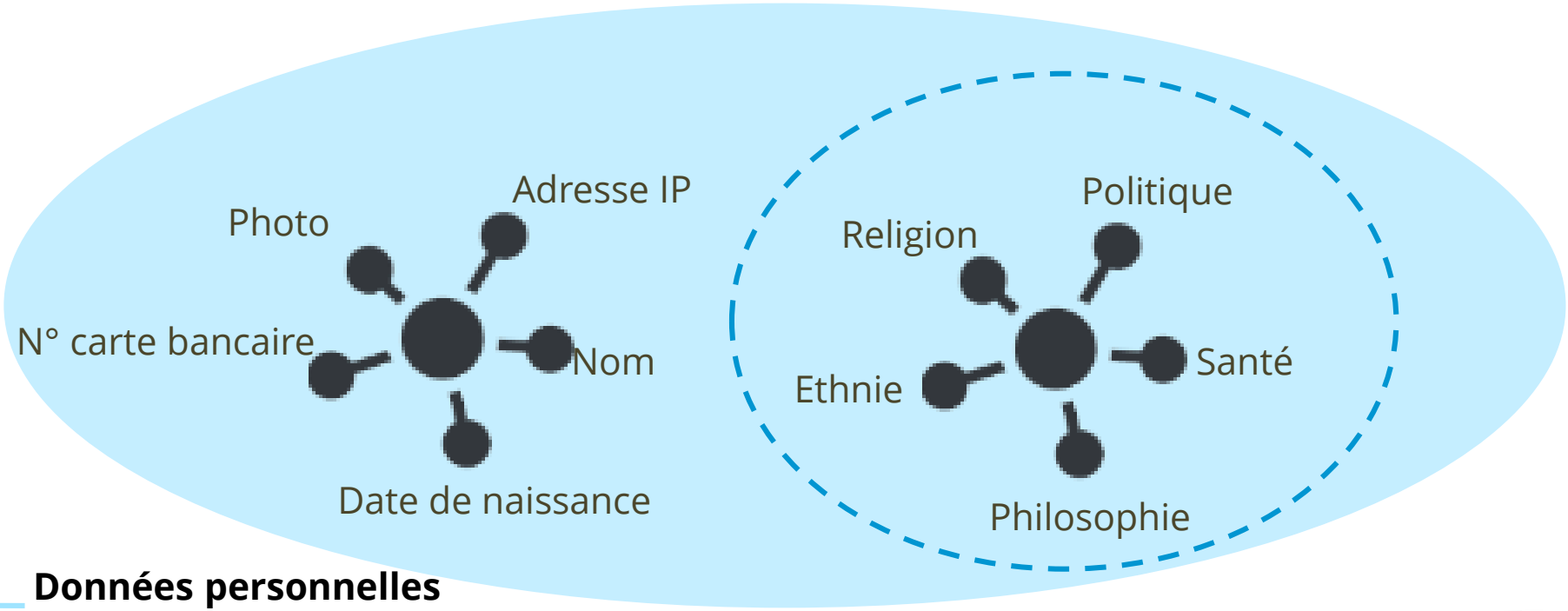
Président du Cluster des entreprises du numérique

Directeur de l'agence skazy

cci
NOUVELLE-CALÉDONIE

Ce qu'il faut retenir du RGPD

Le Règlement Général sur la Protection des Données impose aux organismes publics et privés de se focaliser d'avantage sur l'importance de la donnée personnelle. La donnée personnelle est un actif stratégique, que l'entreprise, dans le cadre de son exploitation, doit protéger.

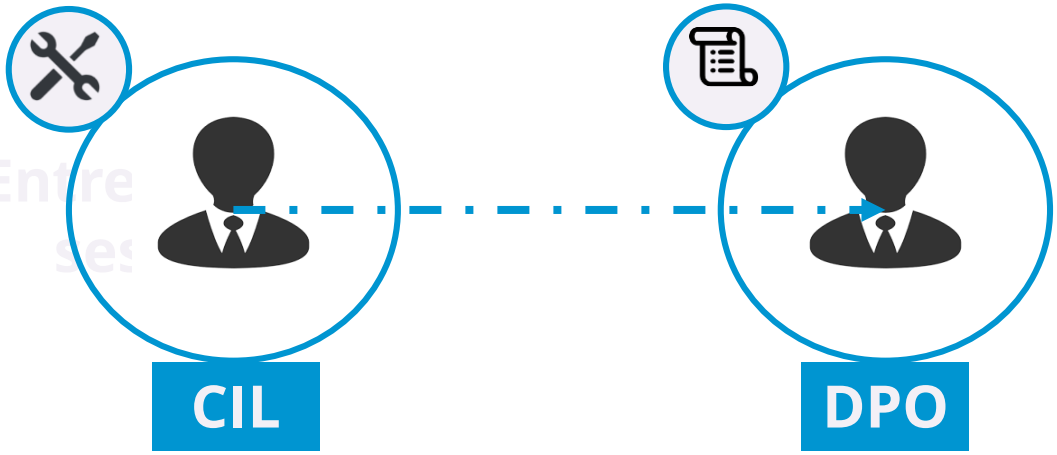


Données personnelles
Données sensibles

Une petite précision sur le profil DPO

D'un profil plus juridique que technique, le **D**élégué à la **P**rotection des **D**onnées devient obligatoire* et intervient pour remplacer le **C**orrespondant **I**nformatique et **L**iberté :

- Former et conseiller les opérateurs de traitement des données
- Contrôler le respect du RGPD et des procédures internes
- Être l'interlocuteur privilégié de l'autorité de contrôle (CNIL)

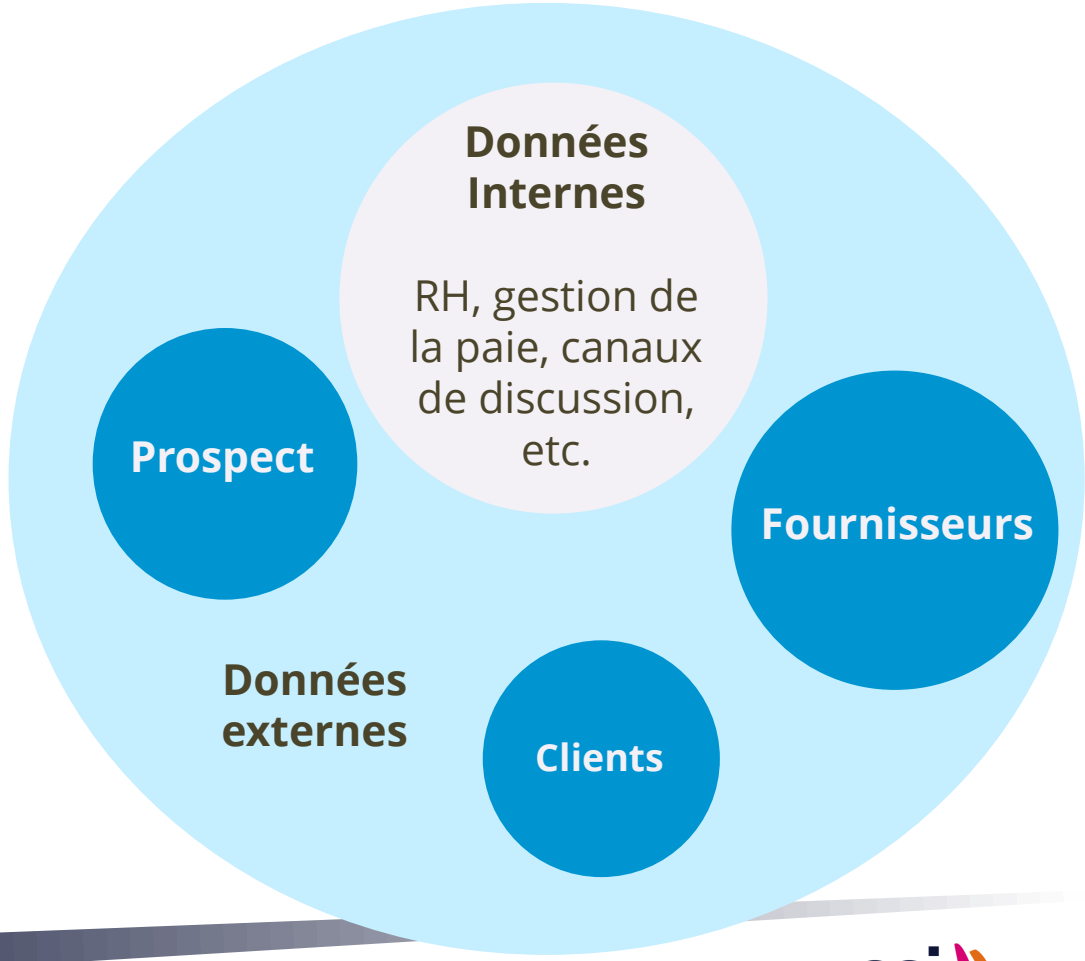


*Obligatoire pour les entreprises ayant plus de 250 salariés, les organismes et les entreprises publiques et lorsque la gestion des données personnelles exige un suivi régulier et systématique à grande échelle des personnes concernées.

Quelles données sont concernées ?

Le RGPD s'applique à **tout organisme public ou privé qui traite des données personnelles**, dès lors qu'il est établi sur le territoire de l'Union européenne ou que son activité cible des résidents européens.

Le RGPD touche aussi bien des traitements de **données internes** que **externes**.



Notre rôle de sous-traitant

Le sous-traitant devient « co-responsable » au côté du responsable de traitement.

1

Informer, assister et alerter

- Accompagnement tout au long du projet de mise en conformité
- Mise en relation avec les interlocuteurs spécialisés si nécessaire
- Sensibilisation sur les enjeux et les risques du RGPD

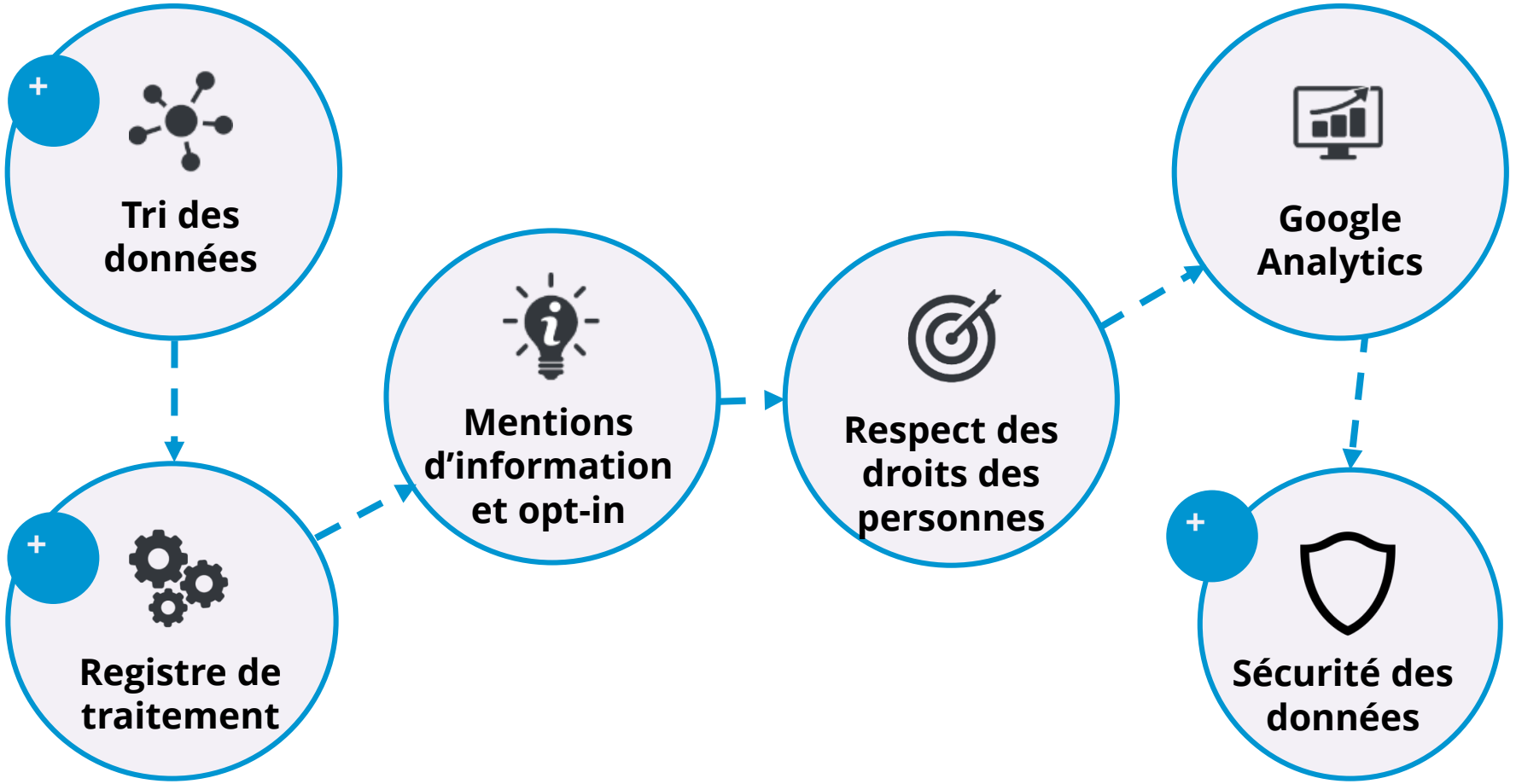
2

Mettre en place des solutions techniques

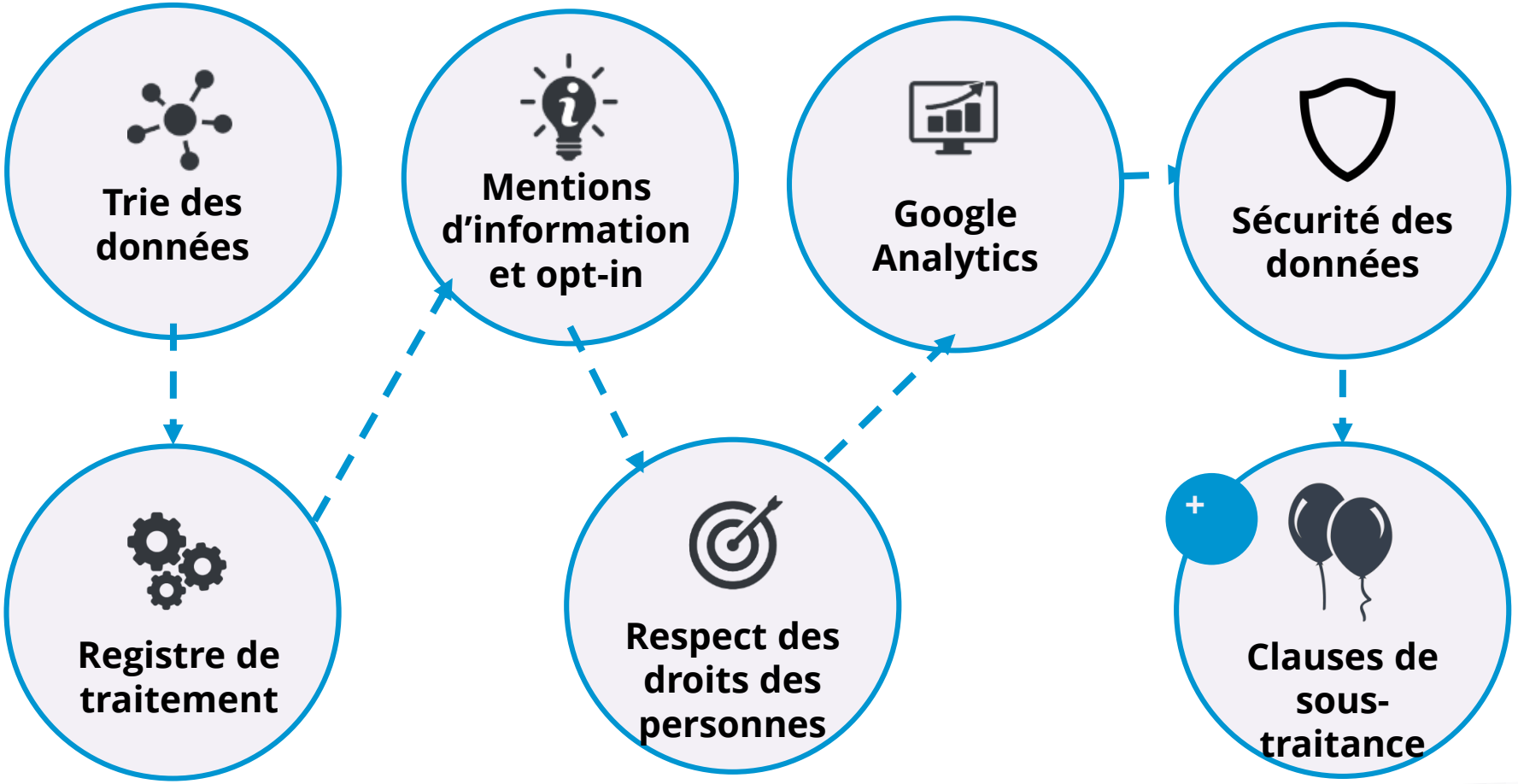
- Création d'emailings, de landing pages et de pages web obligatoires
- Élaboration de scénarios automatisés
- Campagne de consentement, création et adaptation des signatures
- Traitement des demandes
- HTTPS et sécurisation des comptes
- Stockage et traitement des données

J’ai un site vitrine

Je collecte et j'envoie une newsletter



J’utilise plusieurs bases (SaaS, ecommerce)



Typologie de besoin et mise en conformité

1

- J'ai un petit commerce physique
- Je n'émets pas de facture
- Je n'ai pas de site web

Total : 1 à 2 heures

2

- J'ai un petit commerce physique
- J'émets des factures
- J'ai un site vitrine

Total : quelques heures

3

- J'ai un site e-commerce
- J'envoie des newsletters
- J'ai une base CRM

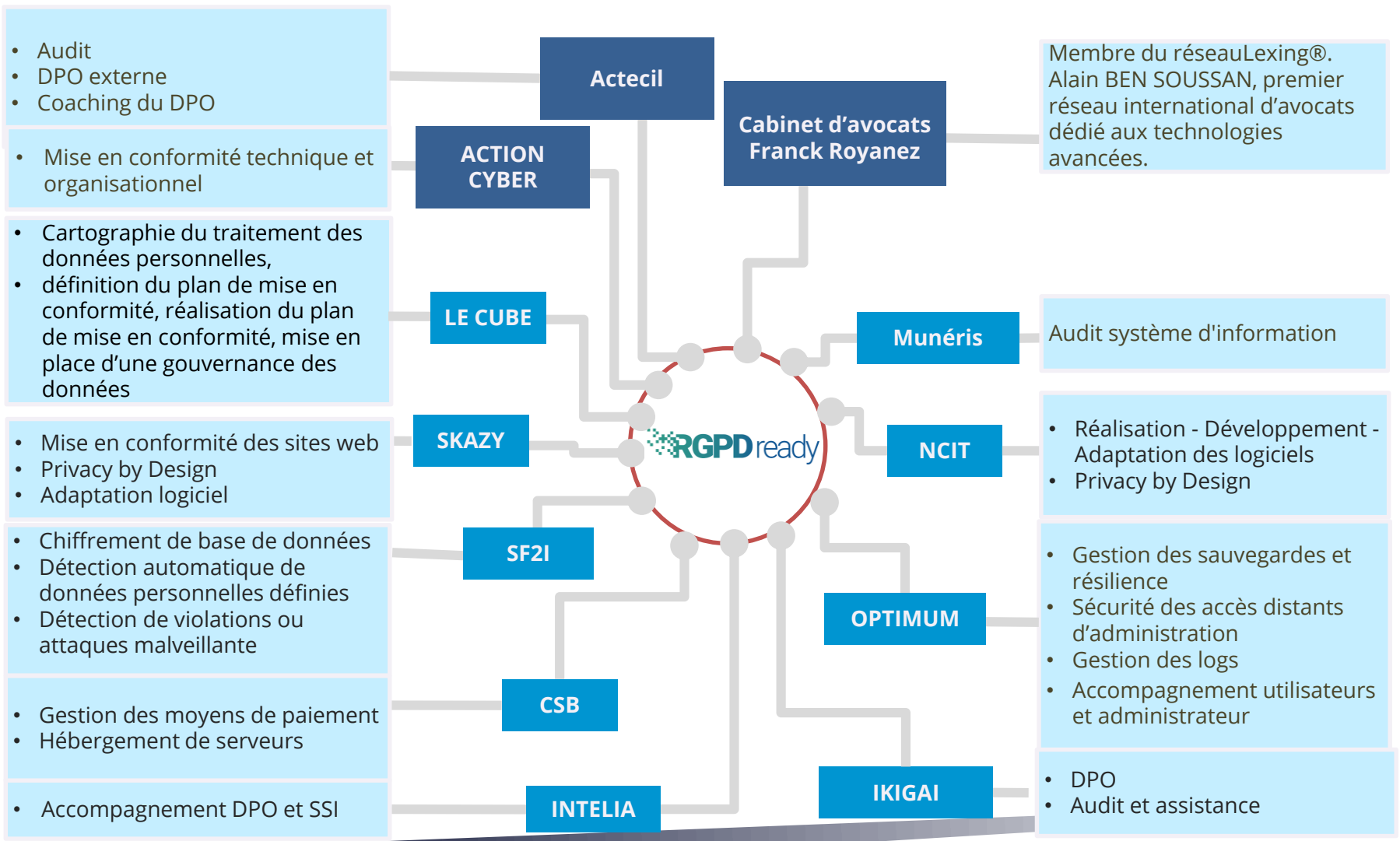
Total : quelques jours

4

- J'ai une PME
- J'ai plusieurs bases de données internes et externes

Total : à partir de plusieurs dizaines de jours et plus si données sensibles

Cartographie OPEN



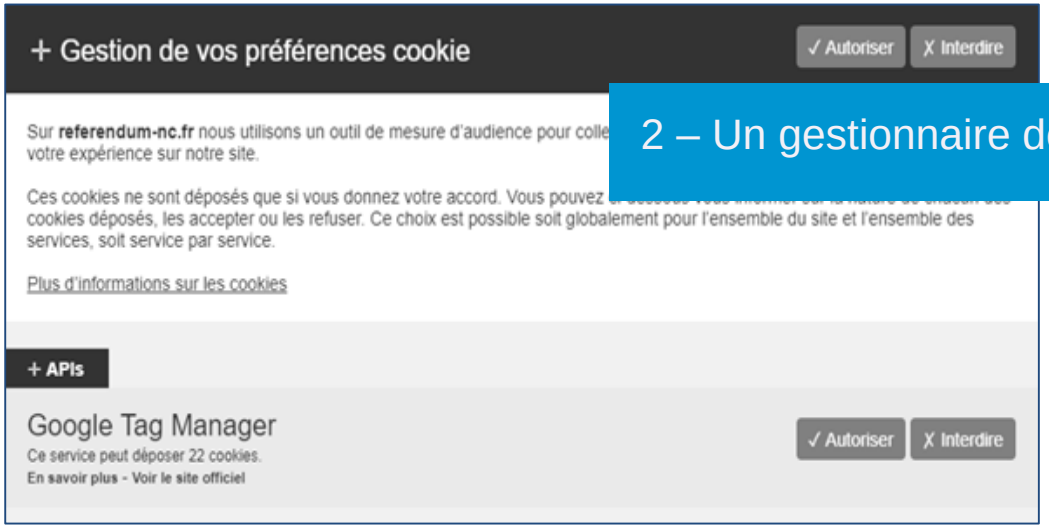
Exemple de mise en place par la société Skazy

1 – Un bandeau cookie

En poursuivant votre navigation, vous acceptez le dépôt de cookies destinés à mesurer la fréquentation du site et à améliorer votre expérience utilisateur. Gestion des préférences cookie

J'ai compris

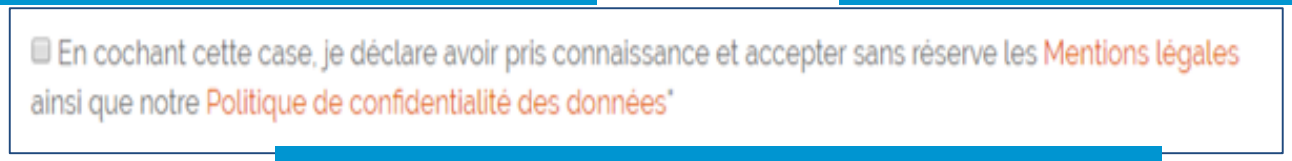
Exemple de mise en place par la société Skazy



2 – Un gestionnaire de cookies

3 – Un opt-in pour formulaire

4 – Une page Mentions légales



5 – Une page Protection des données

Des contraintes et des opportunités

Contraintes

- Application d'une obligation légale
- Investissement financier et humain
- Révision des systèmes d'information et des processus opérationnels
- Documentation et traçabilité des données
- Modification des stratégies marketing et communication

Opportunités

- Meilleure sécurisation et gouvernance des données
- Augmentation de la confiance entre les parties
- Qualification de sa base de données
- Création d'un marché substantiel pour les acteurs du numérique

Diane Rodriguez

Chef du service juridique

INCIDENCES DU RGPD

Témoignage de l'Office des Postes et Télécommunications de Nouvelle-Calédonie

LE MONDE À PORTÉE DE MAIN
www.opt.nc

Comment l'OPT-NC a commencé à se mettre en conformité ?

ACTIONS MISES A JOUR OU NOUVELLES SUITE AU RGPD

Tableau d'archivage et de conservation des données

Refonte du clausier informatique et liberté

Revue des traitements de données personnelles et mise à jour du registre

Création d'une politique de protection des données à caractère personnel

Mise en conformité des sites internet

OPT Nouvelle-Calédonie
LE MONDE À PORTÉE DE MAIN
www.opt.nc

CHANTIERS EN COURS

- Nomination d'un DPO en remplacement du Cil
- Création et documentation de la procédure de violation des données
- Mise en conformité des formulaires de collecte et des contrats clients / sous-traitants
- Insertion du volet RGPD dans la gestion de projets
- Formation / sensibilisation des personnels (e-learning et en présentiel)

OPT Nouvelle-Calédonie
LE MONDE À PORTÉE DE MAIN
www.opt.nc

COMMENT MODIFIER SES CONTRATS CLIENTS ?

RGPD : focus sur nos obligations supplémentaires d'information

Points importants à préciser :

- **La finalité du traitement des données : POURQUOI ?**

Ex : aux fins d'amélioration du parcours client

- **Les acteurs internes concernés : QUI ?**

- **Les types de données : QUOI ?**

- **La durée de conservation des données : COMBIEN DE TEMPS ?**

- **Les droits du client : accès, rectification, effacement, opposition, limitation et portabilité**

COMMENT MODIFIER LES CONTRATS AVEC LES SOUS-TRAITANTS ?

Nouveauté du RGPD : la co-responsabilité

1. Faire un rappel des définitions
2. Indiquer la finalité du traitement des données
3. Préciser le type de données concernées
4. Rappeler les droits des personnes concernées par le traitement
5. Préciser la responsabilité et l'engagement de conformité des parties au contrat
6. Indiquer si un transfert des données hors UE est prévu

COMMENT MODIFIER LES CONTRATS AVEC LES SOUS-TRAITANTS ?

Lister les droits et obligations des parties au contrat

* Pour le responsable du traitement

- Mesures techniques et d'organisation appropriées et effectives
- Mesures de sécurité adéquates
- Sous-traitants présentant des garanties suffisantes en terme de sécurité et de confidentialité
- Coopération en cas de saisine de la CNIL ou demande d'une personne concernée par le traitement de données
- Tenue d'un registre de traitement

* Pour son cocontractant

- Traitement des données exclusivement pour le RT
- Tenue d'un registre des traitements pour le compte du RT
- Aide à la charge de la preuve et coopération
- Obligation de notification en cas de violation de données

MERCI DE VOTRE ATTENTION

Retrouvez l'intégralité de cette présentation dès demain sur
www.cci.nc

Toute l'actualité de la CCI-NC sur :