

RGPD

Préparez votre entreprise



EcoNum
Cellule Économie Numérique

CABINET D'AVOCATS FRANCK ROYANEZ

OPEN
Nouvelle-Calédonie
Organisation des Professionnels de l'Économie Numérique





Moehau Huioutu

Chargée d'études juridiques

Clé n°1 : compétence de l'État

Compétence de l'État :

- ▶ Répartition des compétences prévue par la loi organique du 19 mars 1999

But de la loi informatique et libertés : protéger la vie privée

- ▶ Domaine de la garantie des libertés publiques

Déterminer l'application des textes métropolitains en NC dans le domaine de l'informatique et des libertés

Clé n°2 : Loi informatique et libertés

Textes de référence :

- ▶ Loi informatique et libertés du 6 janvier 1978
- ▶ Décret d'application du 20 octobre de 2005

Autorité de référence :



Clé n°3 : RGPD

Réforme de la réglementation informatique et libertés dans l'Union européenne

- ▶ Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

But :

- ▶ **Mieux protéger les données personnelles** face aux GAFA

Entrée en vigueur en Métropole :

- ▶ 25 mai 2018

Application en NC ?

Application en NC :

- ▶ RGPD ?
- ▶ Loi du 20 juin 2018 relative à la protection des données personnelles ?

Mille-feuille juridique...



Clé n°4 : communiqué de la CNIL

13 juillet 2018 : diffusion d'un communiqué de presse de la CNIL **Application de la loi informatique et libertés en NC**

- ▶ Le RGPD ne s'applique pas
- ▶ La loi informatique et libertés s'applique dans sa version antérieure au 25 mai 2018

Clé n°5 : une ordonnance pour étendre et adapter

Article 32 loi du 20 juin 2018 :

- ▶ Future application de la réforme de la protection des données personnelles en NC

Comment ?

- ▶ Adoption d'une ordonnance par le gouvernement central dans un délai de 6 mois

Objectif :

- ▶ Appliquer et adapter le nouveau cadre juridique aux collectivités d'Outre-mer et notamment la NC

Pour résumer...

Au plus tard le 20 décembre 2018 :

- ▶ Adoption d'une ordonnance en Métropole

Application de la nouvelle réforme européenne informatique et libertés en NC



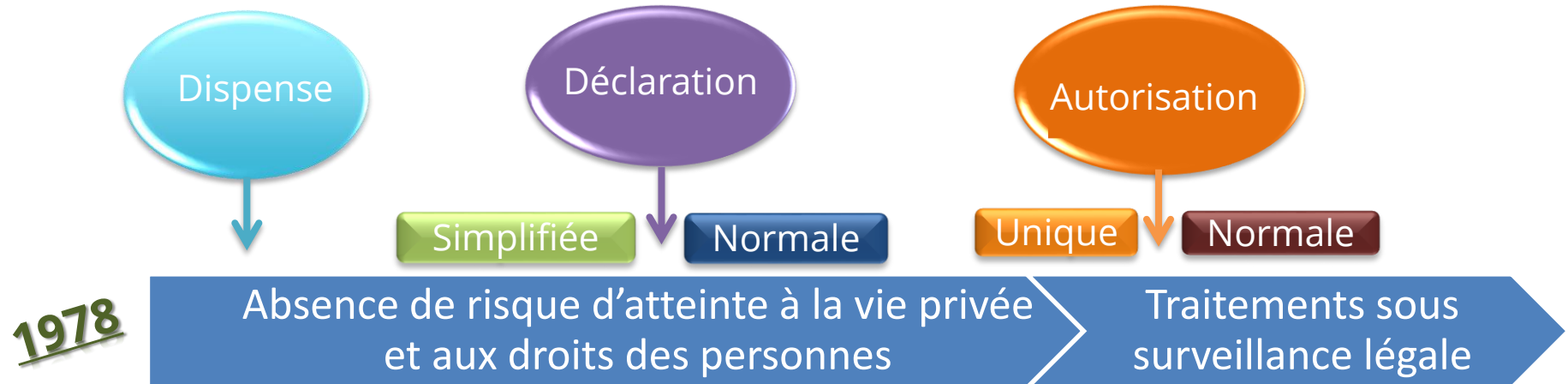
CABINET D'AVOCATS FRANCK ROYANEZ

Franck Royanez

**Avocat à la Cour
Ancien Bâtonnier**



Le RGPD : de la disparition des formalités à la responsabilité



RGPD

Principe général : la responsabilisation

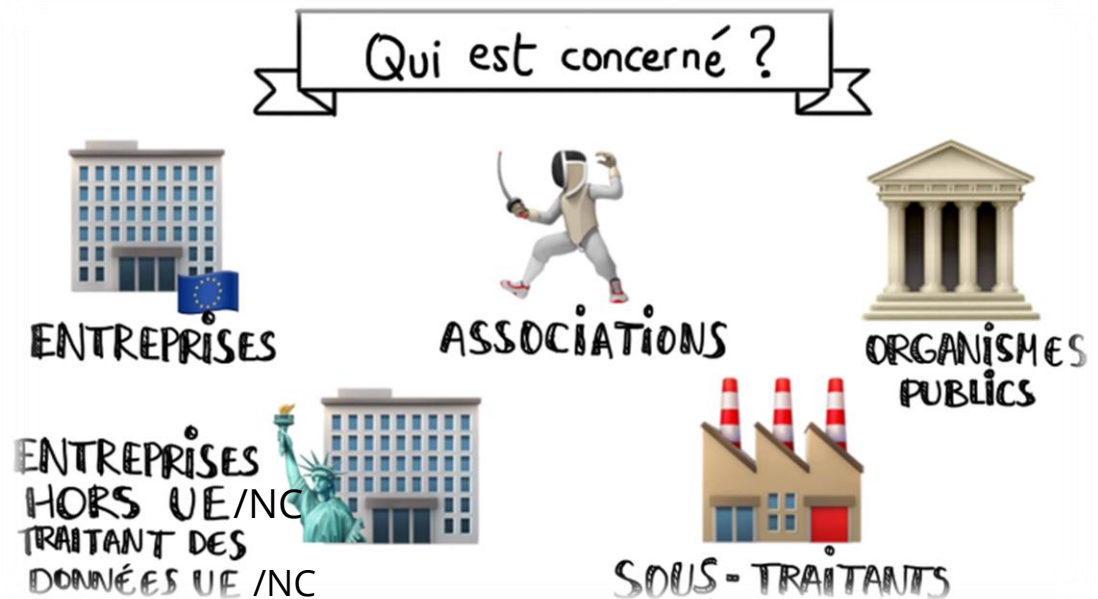
Avec le RGPD, le traitement doit être en conformité avec ses dispositions et le responsable doit être en mesure de démontrer cette conformité.



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



Le délégué à la protection

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



Les services opérationnels

- RH
- DSI
- COMMERCIAUX
- MARKETING...



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

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 *



ETAPE 1

DESIGNER UN PILOTE

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



| Les étapes

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.

ETAPE 2
CARTOGRAPHIER

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.

Réviser 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.).

Concrètement, l'entreprise :

ETAPE 5 **ORGANISER**

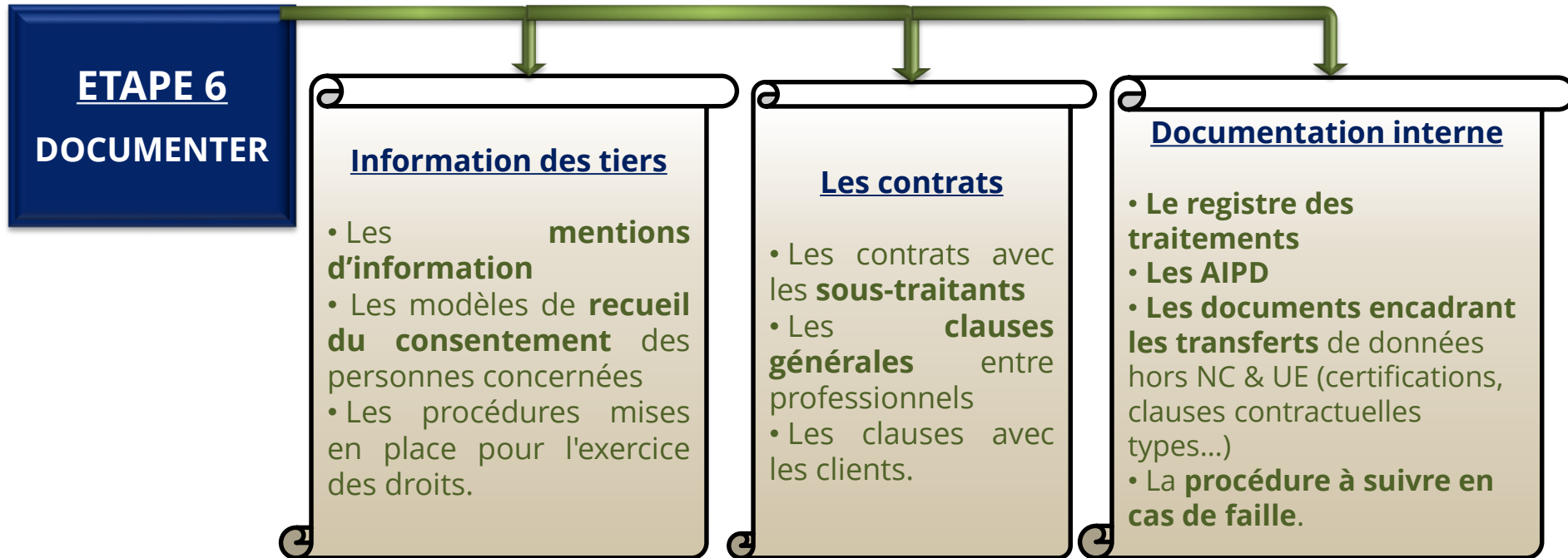
- **Met en place la protection dès la conception** d'un traitement : minimisation de la collecte de données, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données.
- **Organise la remontée d'information** : formation, responsabilisation 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.



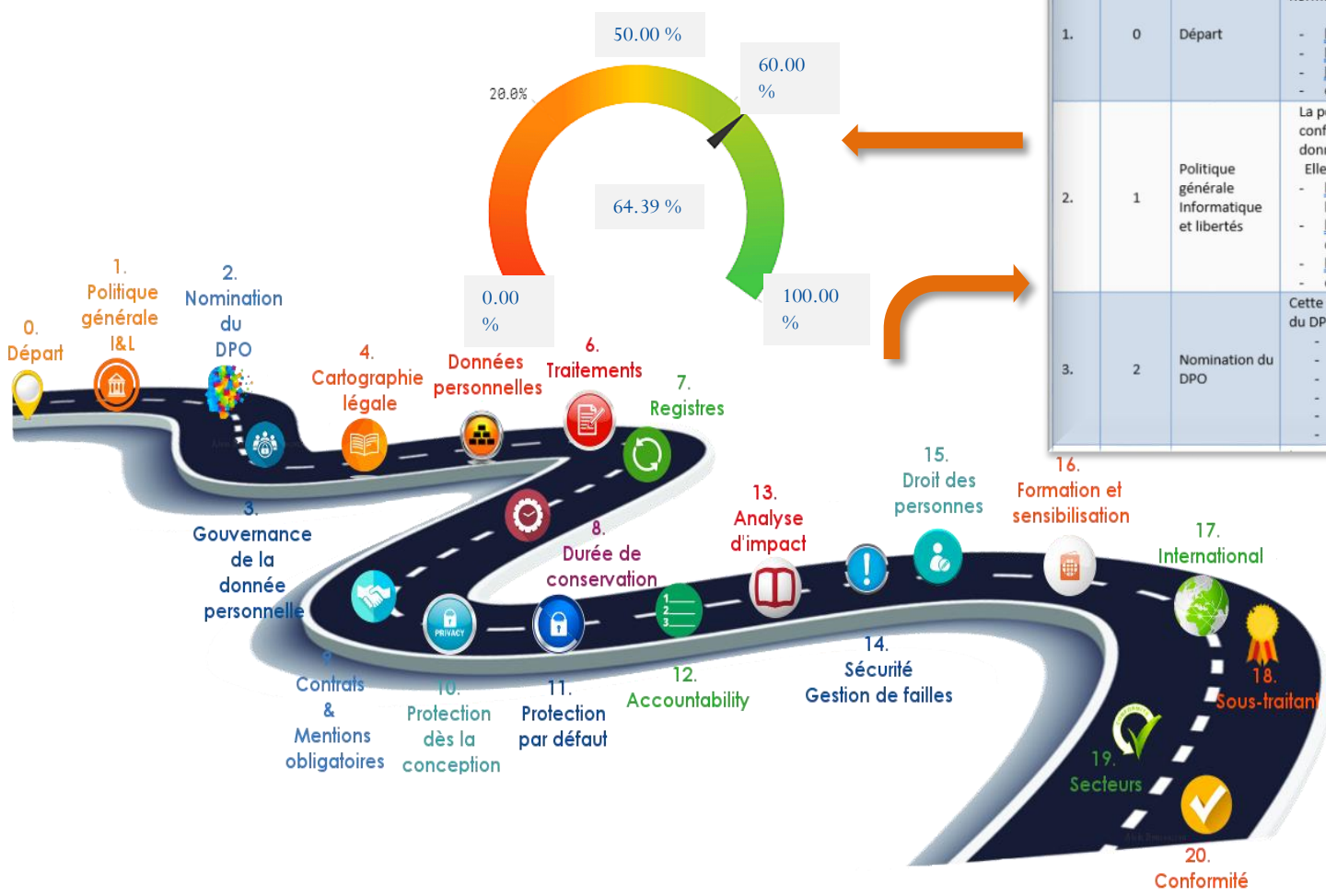
Les étapes

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.



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



QUESTIONS

ÉTAPE 1
DÉSIGNER
UN PILOTE

ÉTAPE 2
CARTOGRAPHIER

ÉTAPE 3
PRIORISER

ÉTAPE 6
DOCUMENTER

ÉTAPE 5
ORGANISER

ÉTAPE 4
GÉRER LES
RISQUES



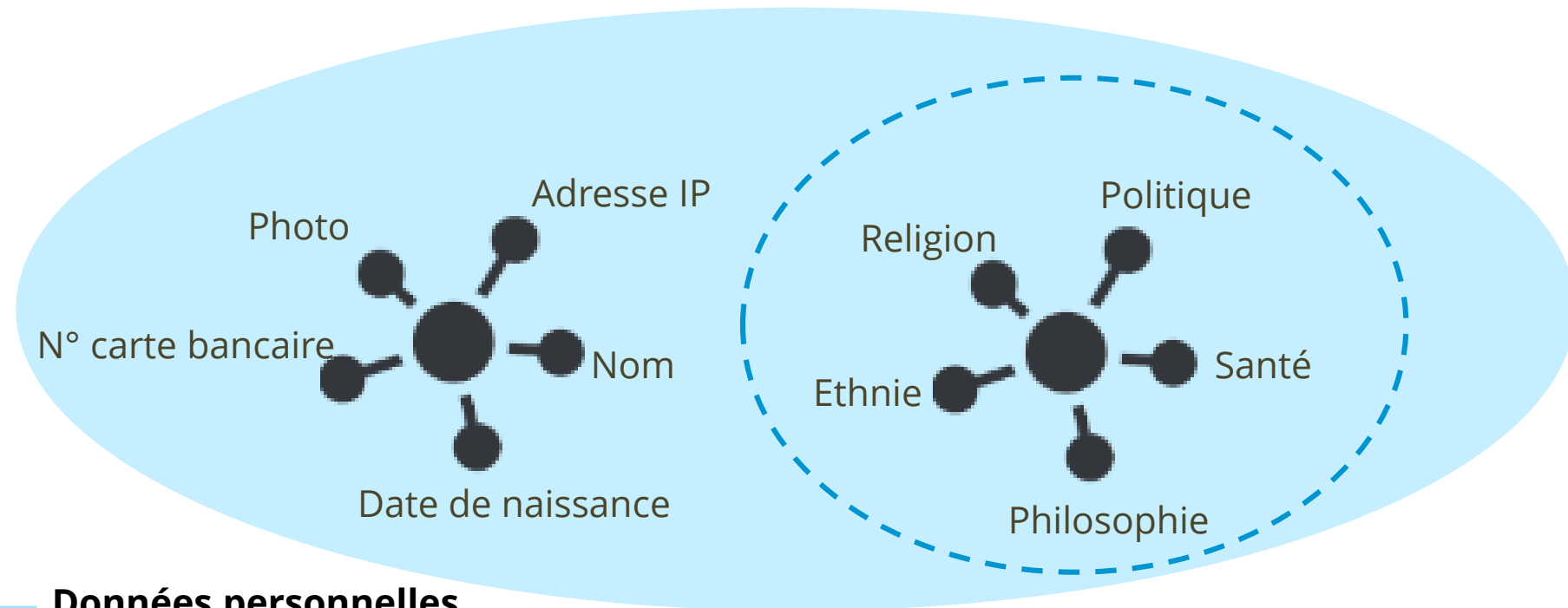
Hatem Bellagi

**Président du Cluster
des entreprises du numérique**

Directeur de l'agence Skazy

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.

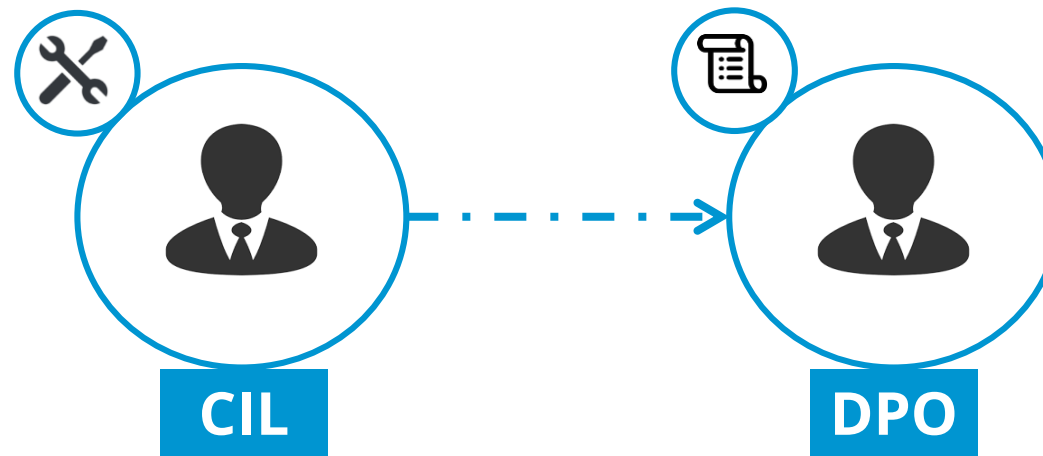


- Données personnelles
- - Données sensibles

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)

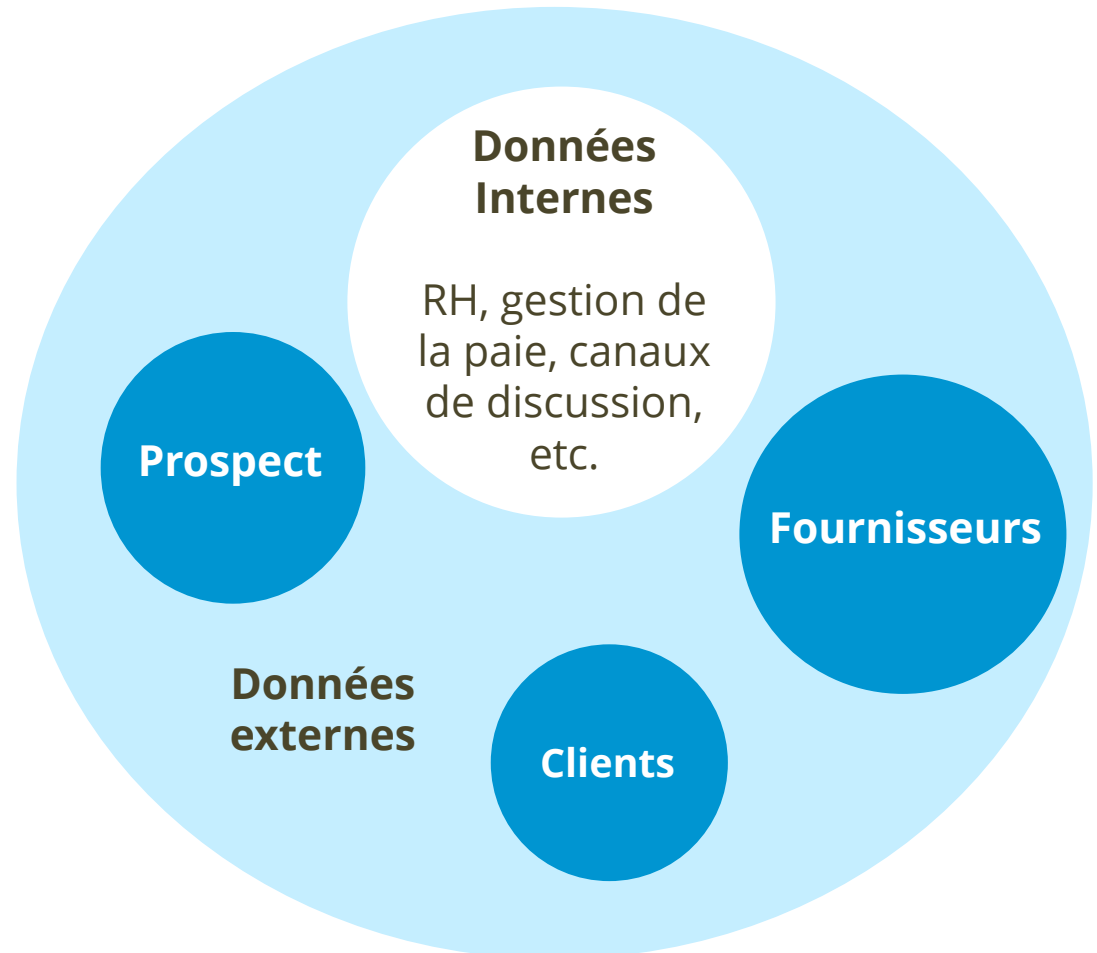


*Obligatoire pour les entreprises ayant plus de 250 salariés, les organismes et les entreprises publiques et lorsque la gestion des données personnelles exige un suivi régulier et systématique à grande échelle des personnes concernées.

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.

Informer, assister et alerter

1

- 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

Mettre en place des solutions techniques

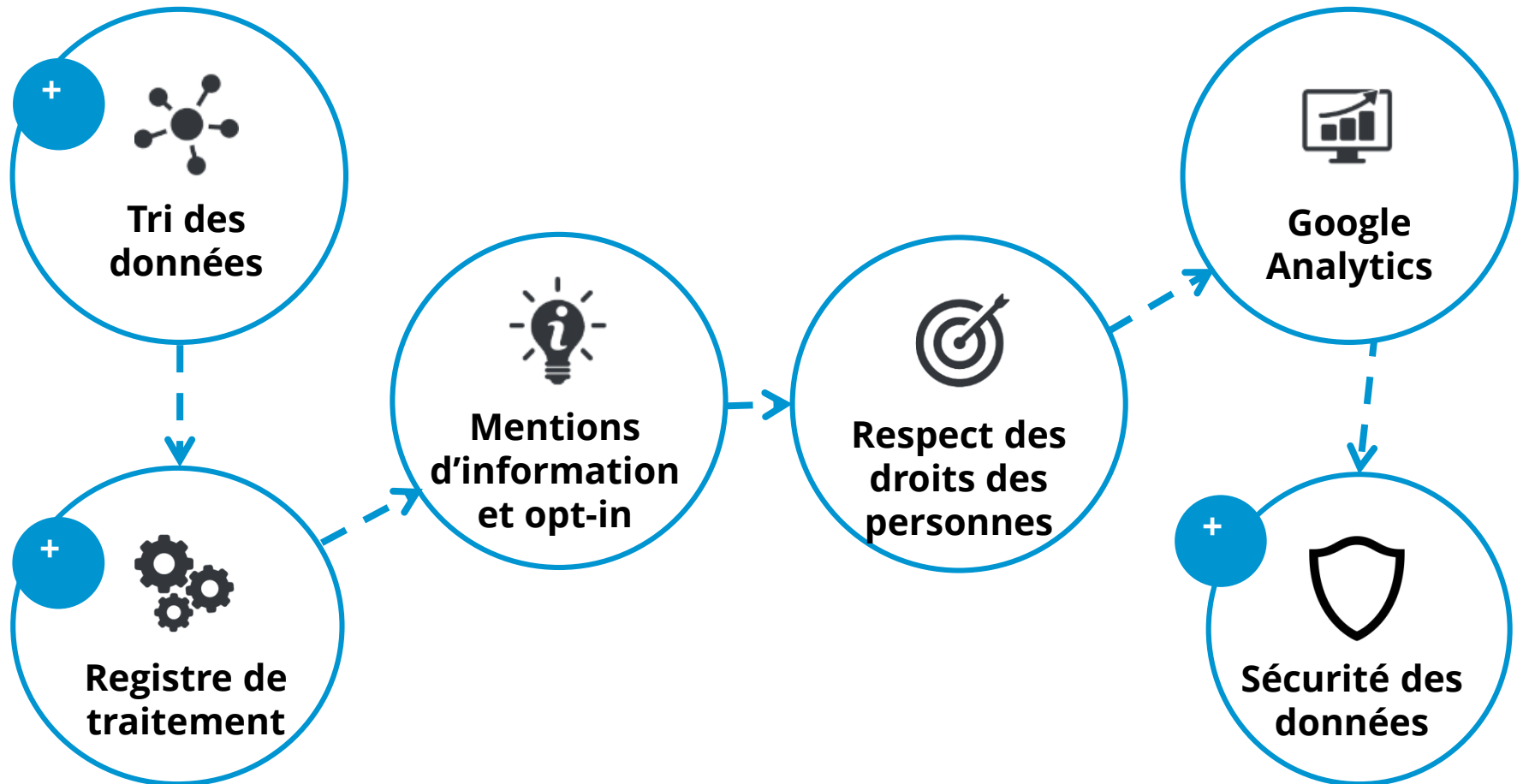
2

- Création d'emails, 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

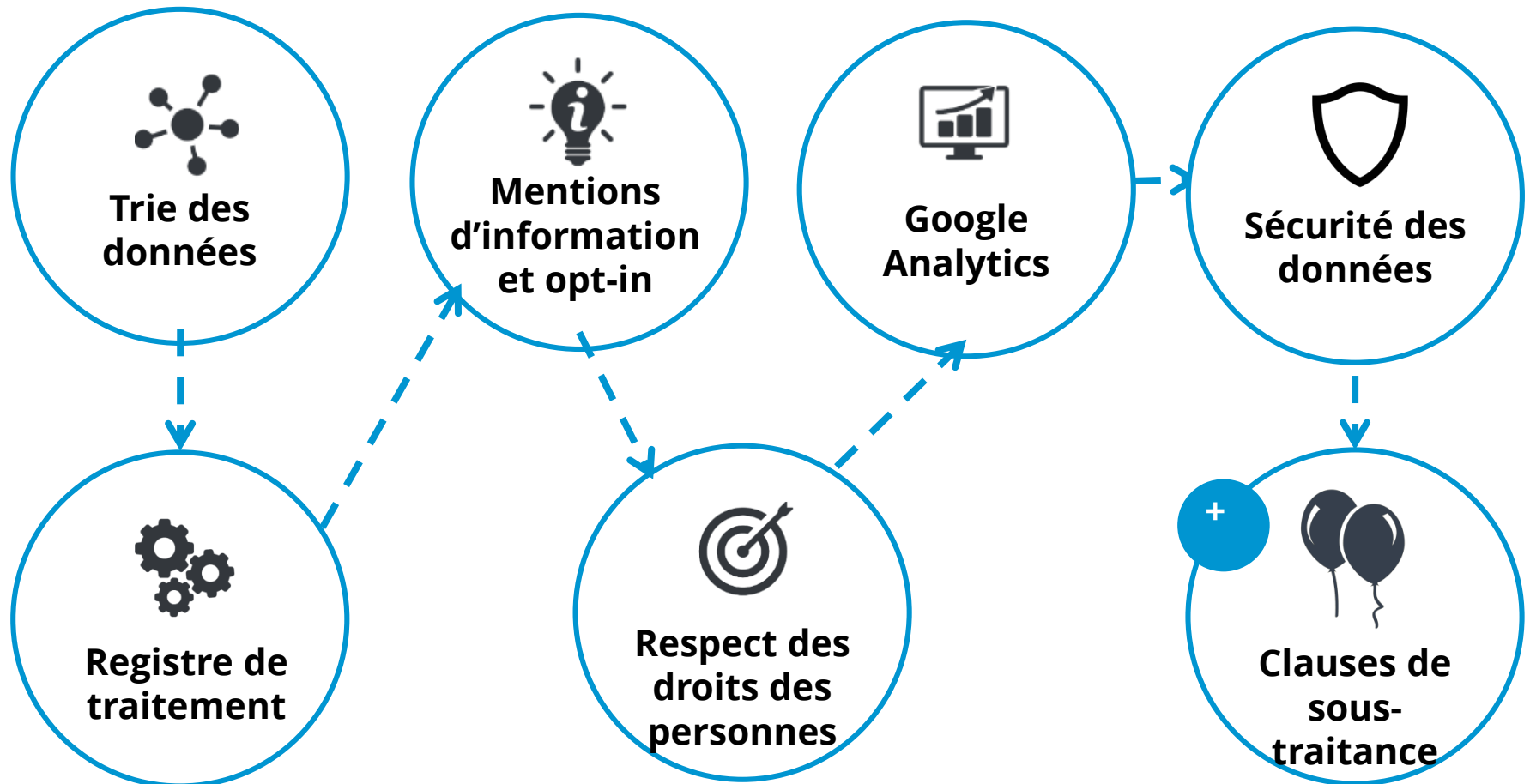
J'ai un site vitrine



Je collecte et j'envoie une newsletter



J'utilise plusieurs bases (SaaS, e-commerce)



Typologie de besoin et mise en conformité

1

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

Total : 1 à 2 heures

2

- J'ai un petit commerce physique
- J'émet 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

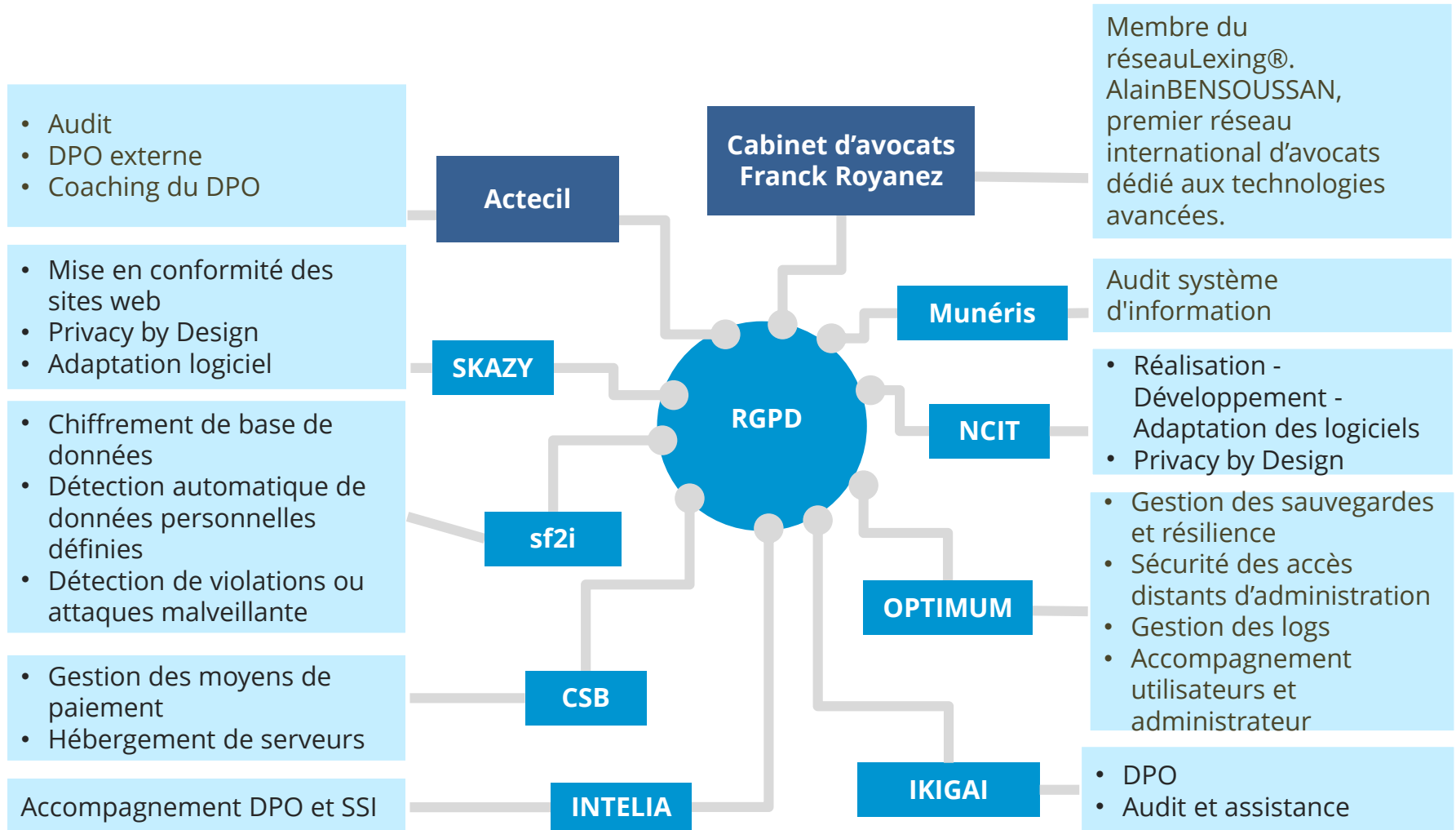
Total : quelques jours

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



Quelques outils mis en place chez Skazy



HISTOIRE & ENJEUX | **ÉLECTEURS** | PROCURATIONS | BUREAUX DE VOTE DÉLOCALISÉS | ACTUS | f



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

Quelques outils mis en place chez Skazy

+ Gestion de vos préférences cookie ✓ Autoriser X Interdire

Sur [referendum-nc.fr](#) nous utilisons un outil de mesure d'audience pour améliorer votre expérience sur notre site.

Ces cookies ne sont déposés que si vous donnez votre accord. Vous pouvez gérer vos cookies déposés, les accepter ou les refuser. Ce choix est possible soit globalement pour l'ensemble du site et l'ensemble des services, soit service par service.

[Plus d'informations sur les cookies](#)

+ APIs

Google Tag Manager ✓ Autoriser X Interdire

Ce service peut déposer 22 cookies.
En savoir plus - Voir le site officiel

2 – Un gestionnaire de cookies

3 – Un opt-in pour formulaire

En cochant cette case, je déclare avoir pris connaissance et accepter sans réserve les **Mentions légales** ainsi que notre **Politique de confidentialité des données***

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

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

MISE À JOUR DES ACTIONS DÉJÀ EN PLACE

- Tableau d'archivage et de conservation des données
- Refonte du clausier informatique et liberté
- Procédures de gestion de projets
- Registre des traitements

CHANTIERS EN COURS SUITE AU RGPD

- **Insertion de l'étude d'impact**
- **Création d'une politique de protection des données à caractère personnel**
- **Mise en conformité des sites internet**
- **Création et documentation de la procédure de violation des données**
- **Formation**

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 ses 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 termes 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 :

