NOOSCOPE

RGPD : Contrainte ou opportunité ?

Marie-Françoise COMBAZ

NOOSCOPE SAS
mfc@nooscope.com - 06 81 06 30 24
www.nooscope.fr

3 juillet 2019
Journée du conseil
Chambre Professionnelle du Conseil-LR

NOOSCOPE

- Un exemple : du diagnostic à la mise en place d'une démarche collective d'amélioration continue des fonctionnements — Exemple
- En quoi êtes-vous concerné ? quelques points clés de la réglementation — Le RGPD
- Quelles questions se poser ? ou comment aller à l'essentiel pour votre activité — Vous et le RGPD
- Comment démarrer ? initier le changement et le pérenniser — Initier et pérenniser

NOOSCOPE

Un exemple concret mené avec le cabinet Garouda

Exemple

- Du diagnostic à la mise en place d'une démarche collective d'amélioration continue des fonctionnements
  - Deux lieux :
    - ⇨ une mission locale pour les jeunes, 6 établissements
    - ⇨ Une agglomération
  - La durée : 4 à 6 mois
  - La mission :
    - ⇨ diagnostic de la situation vis-à-vis du RGPD
    - ⇨ sensibilisation des services
    - ⇨ proposition de plan d'actions

NOOSCOPE

La réalisation

Exemple

- 3 axes de diagnostic

Organisationnel / fonctionnel	Juridique	Technique
• Quels traitements nécessitent une fiche dans le registre ? • Quels traitements nécessitent une analyse d'impact ? • Quels traitements présentent un risque et nécessitent une révision / écriture de process et règles ? • Dans chaque service, quels sont les risques spécifiques ? Quelles sont les mesures de prévention ? • Quel DPO ? Quels responsables de traitements ?	• Quels recueils de données personnelles nécessitent une information / une demande de consentement ? • Quels contrats avec les sous-traitants nécessitent une clarification des responsabilités RGPD ? • Les chartes informatiques intègrent-elles le RGPD ?	• Quels sont les points du SI nécessitant une amélioration de la sécurisation des données personnelles ?

NOOSCOPE

La méthode : rigueur et participation des équipes

Exemple

Cadrage

- Enjeux, objectifs de la mission,
- Services pilotes ou sensibles et personnes référentes

Lancement

- Sensibilisation au RGPD : les données personnelles, les risques, …
- Présentation du déroulement, méthodologie, planning,
- Initialisation du registre des traitements.

Analyse

- Les services : missions, activités, traitements, DP, flux de données, consentement, contrats,
- Les services : analyse des risques, des solutions en place et à mettre en place.

Conclusions

- État des lieux,
- Diagnostic sur tous les points étudiés,
- Priorités,
- Pistes pour un plan d'action.

Restitution

- Présentation,
- Ajustements et rapport final.

Les résultats

Exemple

Le registre des traitements	• La liste exhaustive est faite • Les principaux renseignements utiles sont saisis
Un tableau de bord	• Par service, les traitements nécessitant d'être présents dans le registre, nécessitant une analyse d'impact, présentant un risque particulier, …
Un plan d'action	• Choix des priorités • Choix d'une méthode, d'une organisation • Choix d'un outil
Des équipes mobilisées	• Prise de conscience • Premières mesures initiées • Responsables de traitements repérés et responsabilisés

NOOSCOPE

Les résultats pour les équipes

Exemple

La simplification

- Supprimer les informations inutiles
- Supprimer les documents inutiles
- Mieux gérer la conservation et l'archivage des documents
- Choisir d'utiliser des logiciels standards

La conscience des droits du « client »

- Information, consentement, accès aux données
- Ne faire que ce que l'on doit faire, et savoir pourquoi !

La rigueur

- Sécuriser l'accès physique et informatique aux données
- Limiter et sécuriser les tableaux Excel
- Amélioration de la communication des données personnelles (gestion des mails)

NOOSCOPE

Comment en est-on arrivé là ?

Le RGPD

CNIL
Commission Nationale de l'Informatique et des Libertés

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

6/1/1978
Loi Informatique et libertés
Création de la CNIL

6/8/2004
Modification de la loi
Pouvoirs de la CNIL renforcés

04/05/2016
Publication du RGPD au JO de l'UE

25/05/2016
Entrée en vigueur du RGPD

Période transitoire de 2 ans pour se mettre en conformité

25/05/2018
Application ***directe*** du RGPD

Explosion numérique → extension du domaine de la protection → passage du système déclaratif au principe de ***responsabilisation***

1978

APPLE II

1981

IBM PC

1991
World Wide Web

1998
Google

2004
facebook

2007

Smart Phone

2016

3,9 milliards d'internautes
(± 47 % de la population mondiale)

NOOSCOPE

D'abord, qui est concerné ?

Le RGPD

en tant que citoyen
désireux de protéger les
données le concernant

VOUS

en tant que professionnel
amené à détenir et traiter des
données concernant des tiers

NOOSCOPE

Quels sont les risques ?

Le RGPD

- L’achat de données par les grandes entreprises commerciales,
- Le vol de données ou leur récupération sans qu’il y ait conscience ou accord
- Un problème technique créant une perte de données ou une rupture de la confidentialité
- La réclamation de personnes dont vous détenez les données
- Un contrôle de la CNIL

Des exemples pratiques « sensibles »

- Usage important de dossiers papiers, dont la durée de conservation et l'archivage est géré directement par les personnels de chaque service.
- Usage généralisé de clés usb et de disques durs externes,
- Échanges par mails de dossiers avec les partenaires,
- …

NOOSCOPE

Qu’appelle-t-on « donnée personnelle » ?

Le RGPD

Code	Données personnelles
CIV	État-civil, identification (nom, prénom, adresse, photo, date et lieu de naissance...)
PRS	Vie personnelle (habitudes de vie, situation familiale, etc.)
PRO	Vie professionnelle (CV, situation pro., scolarité, formation, distinctions, diplômes...)
ECO	Infos économiques ou financières (revenus, situation financière, données bancaires...)
CNX	Connexion (adresse IP, log, identifiants, horodatage...)
LOC	Localisation (déplacements, données GPS, GSM …)
NET	Internet (cookies, traceurs, navigation, mesures d’audience …)
AU	Autres catégories de données (préciser) :

NOOSCOPE

Et « Donnée personnelle sensible » ?

Le RGPD

Code	Données sensibles
ETH	Origine ethnique
POL	Opinions politiques
REL	Convictions religieuses ou philosophiques ou appartenance syndicale
GEN	Données génétiques ou biométriques
SAN	Données concernant la santé
SEX	Données concernant la vie sexuelle
PEN	Données relatives aux condamnations pénales ou aux infractions
NUM	Numéro d'identification national unique (NIR ou numéro Séc.Soc)

NOOSCOPE

RGPD : qu'est-ce que ça dit ?

Le RGPD

LÉGITIMITÉ

- Dans quel but ces données sont-elles détenues ?
- Sont-elles limitées à ce qui est indispensable à votre activité ?
- Sont-elles détruites si elles ne sont plus indispensables ?

SÉCURITÉ

- L'accès à ces données est-il correctement protégé ?
- Leur caractère confidentiel est-il affirmé et garanti ?
- Leur intégrité et leur exactitude sont-elles vérifiées ?

RÉVERSIBILITÉ

- Les personnes concernées sont-elles informées ?
- Ont-elles accès à leurs données ?
- Peuvent-elles en demander la modification ou la suppression ?

NOOSCOPE

Vous êtes concerné si …

Vous et le RGPD

- Vous détenez des DP :
  - Celles de vos employés
  - Celles de vos clients, usagers, prospects, partenaires, …

Vous devez nommer un délégué à la protection des données et faire une déclaration à la CNIL …

- « Lorsque le traitement est effectué par une autorité publique ou un organisme public ;
- Lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- Lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions. »

Document CNIL : Lignes directrices concernant les délégués à la protection des données (DPD)

NOOSCOPE

Quels enjeux pour vous ?

Vous et le RGPD

Sécuriser

- Se mettre en conformité avec la réglementation
- Écarter le risque de contrôle (et de sanction) par la CNIL

Optimiser

Transformer la contrainte en opportunité d'amélioration

Anticiper

- Afficher la démarche, en faire un argument
- Se préparer à une interpellation

NOOSCOPE

Nommer un responsable, constituer une équipe

Vous et le RGPD

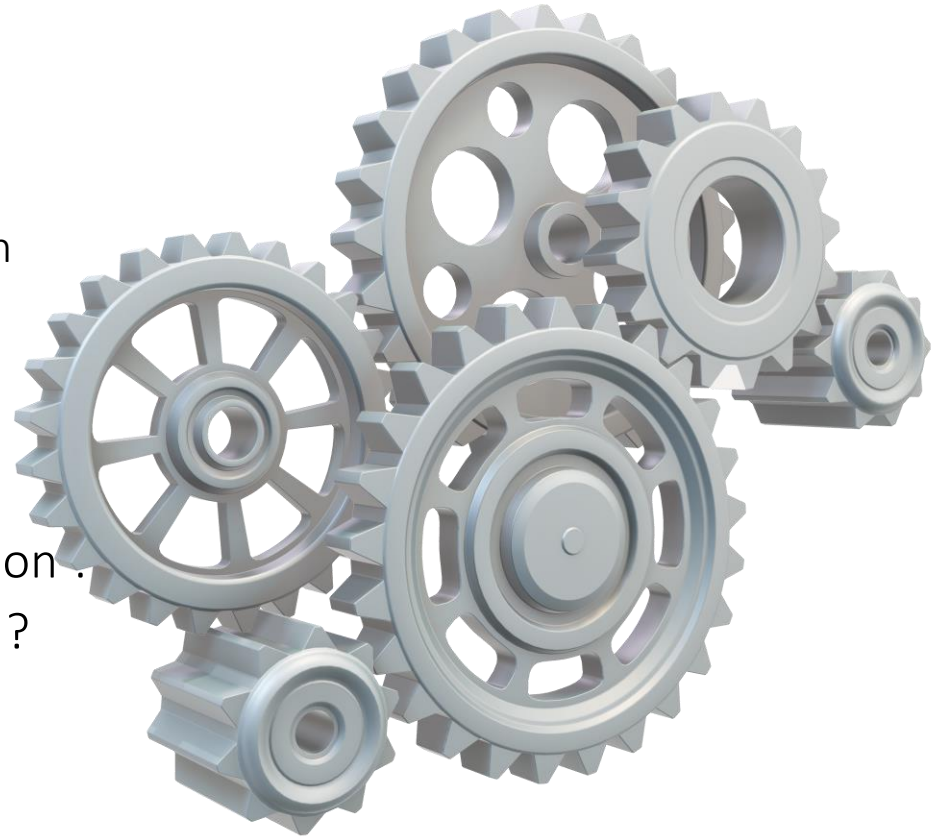
- Des objectifs :
  - Se former, sensibiliser les acteurs du quotidien
  - Une mise en œuvre adaptée à votre situation
- Même non obligatoire la nomination d'un DPD est recommandée
  - Si nécessaire : déclaré à la CNIL,
  - Son rôle :
    - ⇨ « Informer et conseiller le responsable de traitement et ses employés
    - ⇨ Contrôler le respect du règlement européen et du droit national en matière de protection des données
    - ⇨ Conseiller l'organisme sur la réalisation d'une analyse d'impact (DPIA) et en vérifier l'exécution
    - ⇨ Coopérer avec l'autorité de contrôle et être le point de contact de celle-ci »
- Une équipe :
  - Gouvernance : Direction, conseil juridique, DPD, DSI
  - Représentants des métiers : DRH, DAF, services, autres satellites
  - DSI et/ou RSSI (responsable de la sécurité des systèmes d'information)

NOOSCOPE

Préparer la conformité technique du SI

Vous et le RGPD

- Revue de conformité :
  - Identifier les points forts, les non-conformités et les risques
  - Référentiel ANSSI*
- Et en particulier :
  - Où sont stockées les DP ?
    - ⇨ Seuls les hébergeurs européens sont tenus de se mettre en conformité
    - ⇨ Vos supports internes sont-ils sécurisés ?
  - Votre SI est-il protégé contre des actions malveillantes externes ? Comment ?
  - Qui a accès aux DP ? Quelles sont les mesures de protection ?
  - Les mesures mises en place sont-elles efficientes ? À jour ?
  - Quels logiciels sont utilisés ? Qui en a la maîtrise ?
- Identifier les priorités d'action



*Agence Nationale de Sécurité des Systèmes d'Information

NOOSCOPE

Préparer la conformité juridique

Vous et le RGPD

- Mettre en place la documentation interne :
  - ⇨ Chartes informatiques
  - ⇨ Information des personnes, demandes de consentement
  - ⇨ Registre des traitements
- Notifier à la CNIL toute faille de sécurité dans les 72 h à compter de sa découverte
  - ⇨ Prévoir une procédure de signalement
- Imposer les mêmes règles aux prestataires gérant vos DP :
  - ⇨ Sécuriser les contrats avec vos sous-traitants : avenants
  - ⇨ Intégrer les mentions dans les nouveaux contrats

NOOSCOPE

Revoir ses pratiques

Vous et le RGPD

- Quelles sont mes activités ?
- Pour chaque activité :
  - Quel est l'objectif prioritaire recherché ?
  - Quels sont les objectifs secondaires ?
  - Quels sont les traitements, les tâches réalisées qui manipulent des DP ?
  - Quels sont les risques ? Quelles mesures de protection sont-elles en place ?
- Pour chaque traitement :
  - Quelle est sa finalité ?
  - De quel type de personne est-ce que je recueille des données personnelles ?
  - Quelles sont les données personnelles recueillies, traitées ?
  - Où sont-elles ? Quels sont les dossiers, documents, logiciels utilisés ?
  - Avec qui est-ce que je les partage ? Comment ?
  - Comment améliorer la sécurité du traitement ?

NOOSCOPE

Commencer, c’est déjà se mettre en conformité !

Vous et le RGPD

- Consigner tout travail réalisé dans le cadre de la mise en conformité au RGPD
  - Documentation d’ordre juridique
  - Diagnostic technique, mesures prises
  - Registre des traitements
  - Analyses des risques et des mesures de prévention
  - Si nécessaire : Analyses d’impact sur la protection des données personnelles (AIPD)
  - Gestion de projet

NOOSCOPE

Comment initier la démarche ?

Initier et pérenniser

- En parler : chacun est concerné
  - En tant que personne, en tant que professionnel
- Aller voir le site de la CNIL :
  - Tout y est ! les conseils pratiques, les modèles de documents
- Ouvrir un dossier « Conformité RGPD »
  - Les documents actuels
  - Les documents liés à votre démarche,
  - La gestion de projet, les étapes, les déclarations, …
- Regardez ce que vous faites déjà !
  - Et le consigner dans le dossier

NOOSCOPE

Quelles priorités ?

Initier et pérenniser

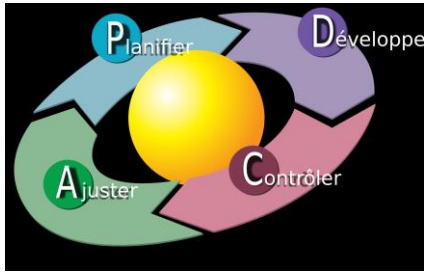
- Monter une équipe capable de décider et d'orienter la mise en œuvre
- Traiter l'aspect juridique :
  - Relativement simple et rapide à mettre en œuvre, vos conseillers habituels vous aideront
  - Sécurisant vis-à-vis des tiers
  - Mettre en place les nouveaux modèles et procédures
- Traiter l'aspect technique :
  - Parce que vous le faites déjà !
  - Les points prioritaires :
    - ⇨ Protections anti-virus, parefeux, …
    - ⇨ Gestion des accès et des mots de passe
    - ⇨ Liste des logiciels utilisés, révision des contrats
  - Mettre en place les nouveaux modèles et procédures
- Faire une revue des activités et traitements :
  - Repérer les activités sensibles
  - Commencer par le diagnostic de ces activités
- Élaborer un plan d'action

NOOSCOPE

Comment pérenniser la démarche ?

Initier et pérenniser

- Pérenniser l'équipe, lui donner les moyens de continuer :
  - Points réguliers :
    - ⇨ Suivi et révision du plan d'action
    - ⇨ Évaluation et améliorations
  - Associer à la démarche qualité ?



- Entretenir le dossier « Conformité RGPD »
- Intégrer la préoccupation RGPD dans tous vos projets :
  - Vous renouvelez ERP, CRM, SIRH, … : vous déléguez au prestataire la sécurité du traitement informatique des données, vous vérifiez les informations saisies, vous organisez les autorisations d'accès, les communications, …
  - Vous installez une GED : vous organisez la conservation des données, les règles d'accès, …
  - Vous achetez un nouvel ordinateur : quelles protections ?
  - Vous embauchez une nouveau collaborateur : comment le former ? Quels codes d'accès lui donnez-vous ?

NOOSCOPE

Merci !

Marie-Françoise COMBAZ

NOOSCOPE SAS
mfc@nooscope.com - 06 81 06 30 24
www.nooscope.fr

Journée du conseil

Chambre Professionnelle du Conseil-LR